

Руководство по установке и эксплуатации

Credit Registry 7.x/8.x

Версия Enterprise

Версия документа: 7.2/29.10.2015

Актуально для Credit Registry Enterprise версии 7.2 и выше

Copyright © 2015 ЗАО "МТЦ"

Лист изменений

Версия/дата	Автор	Комментарии
7.0/13.01.2015	МТЦ	Создание документа
7.1/17.04.2015	Новиков В.	Добавлен раздел “Настройка коннектора Реестр залогов и уведомлений”
7.2/29.10.2015	Лебедь А.	Расширен список доступных сервисов для запросов через Универсальный сервис НБКИ (добавлена возможность запроса кредитного отчета с информационной частью, запроса только информационной части и запроса сервисов Double Data SA/SL)

Оглавление

1 Введение	7
1.1 Термины и определения	7
1.2 Программное обеспечение комплекса	8
1.3 Информационное взаимодействие комплекса	9
1.4 Требования к общесистемному программному обеспечению	9
1.5 Требования к оборудованию комплекса	10
2 Установка Java Runtime Environment (JRE)	11
3 Установка и настройка базы данных	11
3.1 Установка MS SQL Server Express на Windows 7	11
3.2 Установка MS SQL Server	12
3.3 Установка ORACLE	12
3.4 Установка PostgreSQL	13
3.5 Дополнительные утилиты для диагностики и настройки	13
4 Установка Tomcat	14
4.1 Настройка средств диагностики при сбое Tomcat	15
4.2 Настройка памяти Tomcat	15
4.3 Запуск Tomcat	16
5 Соединение Tomcat с базой данных	17
5.1 Проверка корректности данных для соединения с БД	17
5.2 Конфигурация соединения с базой данных	17
5.2.1 Дополнительные настройки	20
6 Развертывание приложения Credit Registry на Tomcat	21
6.1 Установка	21
6.2 Важные рекомендации	22
6.3 Запуск приложения	22
7 Настройка соединения с НБКИ	23
7.1 Настройка шлюза поддержки защищенного соединения для Credit Registry (НБКИ)	23
7.2 Настройка коннектора НБКИ в Credit Registry	23
7.3 Настройка параметров коннектора ФМС	31
7.4 Настройки параметров коннектора ГИБДД	35
7.5 Настройки параметров коннектора ТСЗ	38
7.6 Настройки параметров коннектора НБКИ-БРС	41
7.7 Настройка параметров коннектора статистических отчетов НБКИ	45

7.8	Настройка коннектора НБКИ-AFS	50
8	Настройка соединения с ОКБ.....	53
8.1	Настройка защищенного соединения с ОКБ.....	53
8.2	Настройка коннектора ОКБ в Credit Registry	54
8.3	Настройка сервиса “National Hunter”	58
8.3.1	Подписание соглашения о вступлении в программу “National Hunter”	58
8.3.2	Создание коннектора National Hunter	59
8.3.3	Настройка параметров сервиса	62
9	Настройка соединения с Эквифакс Кредит Сервисиз.....	64
9.1	Настройка защищенного соединения с Эквифакс.....	64
9.2	Настройка коннектора Эквифакс в Credit Registry	65
9.3	Настройка Equifax FPS	71
10	Настройка соединения с БРС	75
10.1	Настройка защищенного соединения с БРС	75
10.2	Настройка коннектора БРС в Credit Registry	76
11	Настройка соединения с ЦККИ	80
11.1	Настройка запросов ЦККИ через почту X400	81
11.2	Настройка запросов ЦККИ через систему СВК	87
11.3	Настройка запросов ЦККИ через каталоги отправки банковской отчетности (подписание и шифрование осуществляется внешним ПО, в частности, ПТК ПСД)	91
11.4	Настройка запросов ЦККИ через каталоги запросов и ответов (подписание и шифрование осуществляется комплексом CRE + SSLGate + SCIGNEX + VerbaOW).....	93
11.5	Настройка запросов ЦККИ через НБКИ.....	95
11.6	Пакетирование запросов ЦККИ.....	97
12	Настройка коннектора СМЭВ ФМС	97
13	Настройка коннектора Реестр залогов и уведомлений	100
14	Настройка прокси-соединения для связи сервера Credit Registry с БКИ (НБКИ, ОКБ, БРС)	103
15	Настройка потоковых запросов.....	104
16	Настройка пакетных запросов.....	106
17	Взаимодействие с IBM WebSphere MQ	108
17.1	Предварительные условия	108
17.2	Настройка WebSphere MQ	108
17.2.1	Создание фабрики соединений	108
17.2.2	MQ-авторизация	110
17.3	Настройка сервера приложений (Tomcat).....	111

17.4	Активация в CRE интерфейса взаимодействия через WebSphere MQ.....	113
18	Типичные ошибки при установке комплекса.....	113
19	Мониторинг работы коннекторов.....	115
19.1	Доступ к данным мониторинга	115
19.2	Overall и Current разделы статистики	115
19.3	Правила именования и значения параметров	116
19.4	Измеряемые параметры и события.....	116
20	Настройка курсов валют.....	118
	ПРИЛОЖЕНИЕ А. Инструкция по установке ключей CryptoPro для SSLGate.....	120
	ПРИЛОЖЕНИЕ В. Рекомендации по установке нескольких копий приложения.....	123
	ПРИЛОЖЕНИЕ С. Установка новых версий приложения.....	124
	ПРИЛОЖЕНИЕ D. Настройка SSLGate для работы с ЦККИ	125
	ПРИЛОЖЕНИЕ E. Установка новых версий SSLGate	130
	ПРИЛОЖЕНИЕ F. Настройки, связанные с изменением временных зон.....	131
	ПРИЛОЖЕНИЕ G. Типичные ошибки настройки коннекторов.....	132
	Ошибка подписи запроса (sign_errors) java.io.IOException: ssl gate error: Certificate S/N:"519a549900020000654c" not found in store. Объект или свойство не найдено.....	132
	Ошибка. Сертификат не найден. Certificate is not found.....	132
	java.io.IOException: HTTP[S] remote request error: HTTP/1.1 403 Forbidden.....	133
	Ошибка. Код отчета 12 Расшифровка кода отчета: Структура XML запроса не корректна.....	133
	java.io.IOException: HTTP[S] remote request error: HTTP/1.1 401 Unauthorized.....	134
	Ошибка. Код отчета 50 при запросе в НБКИ	134
	Ошибка. Код отчета 32. Текст: User Not Found.....	134
	Ошибка: 99 – нет полномочий	135
	Ошибка: Такого отчета не существует.....	135
	Статус: Ошибка Ошибка: Ошибка подписи запроса (sign_errors) Текст ошибки: java.io.IOException: ssl gate error: Getting signed BLOB size failed. Набор ключей не существует	136
	Ошибка Использован незарегистрированный сертификат подписи ("35e1320c0000000014f")	136
	Ошибка подписи запроса (sign_errors) java.net.SocketTimeoutException: Read timed out.....	136
	Ошибка. Код отчета 28	137
	Ошибка. Код отчета 49 при запросе в НБКИ	137
	Ошибка базы данных код ошибки -4 или -6: база данных не подключилась.....	137
	Превышено время ожидания ответа БКИ: read timeout.....	137
	Статус: Ошибка Ошибка: Ошибка соединения с БКИ (bki_conn_errors) Текст ошибки: ru.mbtc.creditregistry.sslgate.SslGateNegotiateException: SSLGate error: Connect SSL client handshake failed.....	138

Статус: Ошибка Ошибка: Ошибка подписи запроса(sign_errors) Текст ошибки: java.io.IOException: ssl gate error: Неправильный открытый ключ поставщика / The Keyset parameter is invalid.....	139
Статус: Ок Ошибка: Ошибка при разборе xml-ответа.....	139
MQ-ошибка в логe stdout: com.ibm.mq.MQException: MQJE001: An MQException occurred: Completion Code 2, Reason 2035.....	139
MQ-ошибка в логe stdout: org.codehaus.xfire.fault.XFireFault: Parameter {http://creditregistry.ru/2010/webservice/SingleFormatService}GroupRequestData does not exist! .	140
С момента выпуска сертификата прошло больше года.....	140
Код ошибки НБКИ 23 Проверка подписи не прошла.....	141
Wrong PIN was presented.....	141
Ошибка: Ошибка соединения с БКИ(bki_conn_errors).....	141
Текст ошибки: ru.mbtc.creditregistry.sslgate.SslGateNegotiateException: SSLGate error: Ошибка вызова SSPI, см. внутреннее исключение. (0x80004005):	141
Ошибка: Ошибка подписи запроса (sign_errors): java.io.IOException: ssl gate error: Getting signed BLOB size failed. Function failed during execution.....	142
ПРИЛОЖЕНИЕ Н. Контакты для связи с БКИ	143

1 Введение

Программный комплекс Credit Registry предназначен для координации работы сотрудников различных подразделений и филиалов банка, а также для обеспечения интегрированной работы сторонних автоматизированных банковских систем и хранилищ данных в процессе выдачи и обслуживания кредитов. Credit Registry обеспечивает автоматизацию процессов взаимодействия банка с кредитными бюро (БКИ), центральным каталогом кредитных историй (ЦККИ) и другими внешними сервисами на рынке потребительского кредитования. Система обеспечивает:

- Интеграцию информационных систем банка и систем поддержки принятия решений в единую централизованную систему хранения, доступа и обработки информации на единой основе и в едином формате данных;
- Интеграцию со средствами БКИ (НБКИ, ЭКС, ОКБ) для автоматического предоставления сведений о кредитных историях субъектов.

Комплекс Credit Registry предназначен для получения, хранения, обработки и передачи данных по запросам смежных систем по заданным критериям и в составе, заданном применяемой схемой XML и функционалом интеграционных сервисов. В рамках Credit Registry решается комплекс задач по получению и обработке данных, поступающих из АС банка, а также подготовке данных и их отправке на сторону ИС БКИ.

Данная документация описывает действия администратора по настройке общесистемного программного обеспечения, требуемого для функционирования комплекса Credit Registry, а также настройки самого программного ядра, исполняющего бизнес логику комплекса. Описываемая версия комплекса – Credit Registry 7.x/8.x. Компоненты комплекса, необходимые для установки и настройки, могут быть получены по ссылке <http://www.creditregistry.ru/download>

1.1 Термины и определения

Термин	Определение
Абонент УЦ	Ответственный абонент автоматизированного рабочего места Пользователя Удостоверяющего Центра
АС	Автоматизированные системы
БД	База данных
БКИ	Бюро кредитных историй
Интеграционная платформа	Программно-аппаратный комплекс, обеспечивающий разработку, функционирование и администрирование интеграционных сервисов

Интеграционный сервис	Логически и функционально целостный комплекс программных модулей, протоколов и регламентов функционирования, обеспечивающий автоматизированное взаимодействие двух и более информационных систем и решающий конкретную задачу интеграции
ИС	Информационные системы, системы электронного документооборота
КИ	Кредитная история
НБКИ	ЗАО «Национальное бюро кредитных историй»
ОКБ	ЗАО «Объединенное кредитное бюро» (ранее Experian-Interfax)
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
ФМС	Федеральная Миграционная Служба
ЭКС	ООО «Эквифакс Кредит Сервисиз»
ЭЦП	Электронно-цифровая подпись
API	Application Programming Interface – программный интерфейс, служащий для взаимодействия двух систем
CRE	Credit Registry (Enterprise) – описываемый данным документом программный комплекс, представляющий сотрудникам и АС банка единую точку входа для взаимодействия с различными БКИ (для отправки информации о КИ, обработки сообщений об ошибках, формирования запросов на получение кредитных отчетов и их последующего хранения)
JRE	Java Platform, Standard Edition, Runtime Environment – виртуальная машина Java, библиотеки классов и другие компоненты, необходимые для запуска апплетов и приложений, написанных на языке программирования Java
TUTDF	Trans Union Transmit Data Format – формат передачи данных в НБКИ
XML	eXtensible Markup Language – расширяемый язык разметки; текстовый формат для обмена структурированными данными между программами

1.2 Программное обеспечение комплекса

Программное обеспечение комплекса подразделяется на целевое и общесистемное:

- к целевому ПО относится Credit Registry, обеспечивающее обработку бизнес-логики;
- к общесистемному ПО относятся программные средства функционирования и управления целевым ПО.

Платформа Apache Tomcat и JRE являются центральным ядром серверной части комплекса, обеспечивающего интеграцию всех частей ПО Credit Registry в единую функциональную модель. Рекомендуемый размер оперативной памяти под сервер, на котором будет установлен Tomcat - 2 ГБ или более. Информационный обмен и взаимосвязь между приложениями обеспечивается с использованием протокола TCP/IP. В протоколах, обеспечивающих доставку данных, используются

связка с XML. На данных протоколах строится базовая модель сервисов, обеспечивающих взаимодействие приложения Credit Registry и внешних приложений.

Основным программным компонентом является сервер приложений Tomcat, обеспечивающий функционирование Credit Registry и обработку запросов к комплексу. Он же является web-сервером, принимает, обрабатывает и пересылает пользовательские запросы серверу приложений и обратно.

Сервер БД используется сервером приложений для процедур хранения, извлечения и обработки необходимых данных. Набор необходимых данных формируется на основе обрабатываемых сервером приложений входящих данных.

1.3 Информационное взаимодействие комплекса

Комплекс Credit Registry предназначен для хранения данных, в том числе получаемых из внешних источников. ПО Credit Registry исполняет всю бизнес-логику по обработке поступающих данных и обработке запросов к данным, в том числе и обеспечение контроля полноты данных о субъекте и кредитных делах.

Предметно-ориентированная информация, составляющая данные о кредитных делах субъектов, предназначенная для хранения в Credit Registry, содержится во входных сообщениях, передаваемых внешними приложениями. Внешние приложения банка взаимодействуют с Credit Registry с использованием интерактивного доступа и интеграционных компонент. Интерактивный доступ реализуется через клиентский Web-браузер. Интеграционные компоненты разрабатываются на стороне банка. Функциональность по контролю и поддержанию корректного формата данных реализуется на стороне внешнего приложения. В Credit Registry данные проверяются на обязательность и их соответствие типам, описанным XML-схемой.

Вся функциональность по контролю и поддержанию корректного состава передаваемых данных для БКИ реализуется на стороне Credit Registry.

Обмен данными между АС банка и ИС БКИ в части запроса кредитных историй и получения отчетов БКИ осуществляется с помощью механизма web-сервисов Credit Registry, реализующего набор функций для передачи запросов к ИС БКИ. Взаимодействие возможно посредством создания клиентов на стороне АС банка, выполняющих запросы к web-сервисам Credit Registry. В части запросов к ИС БКИ Credit Registry работает только с программными интерфейсами БКИ, реализующими вызов функций API БКИ.

1.4 Требования к общесистемному программному обеспечению

Для развертывания программного комплекса Credit Registry на сервере должны быть установлены:

- ОС: MS Windows 7/8.1/10, Windows Server 2008/2008R2/2012/2016/2019. Рекомендуется Windows Server 2016 или более актуальный.
- Java SE (JRE) 1.8.x, JDK 11. Для CreditRegistry 7.x допустимо использовать Java 1.7.x/1.8.x, для CreditRegistry 8.x необходимо использовать Java 1.8.x/11
- Tomcat 8.5.x/9.x (бесплатно, входит в установочный комплект)
- СУБД. Возможны следующие варианты:
 - Для ранних версий CreditRegistry: MS SQL Server 2008, для CreditRegistry начиная с версии 2019.4: MS SQL Server 2012 или выше;
 - Oracle 12.1 или выше. Используется функционал в рамках Standard Edition (т.е. можно использовать и Standard Edition, и Enterprise). Oracle Express Edition не поддерживается.
 - PostgreSQL 10 или выше. Данная версия БД допустима к использованию только для версий из линейки 2022.3.2 и выше.
- При имеющихся технических средствах рекомендуется использовать отдельный сервер для размещения БД либо использовать уже существующий экземпляр MS SQL/Oracle/PostgreSQL
- КриптоПро CSP 4.0 – программный продукт, требующийся для использования https-соединений с БКИ для передачи запросов и получения отчетов о кредитных историях. Необходимость наличия продукта КриптоПро CSP определяется положениями технического регламента БКИ (приобретается у компании КРИПТО-ПРО). Для работы с сертификатами ГОСТ 2012 необходимо использовать КриптоПро CSP 4.0 или 5.0
- .Net Framework 4.5. (.Net Framework 3.5 для работы SSLGate версии 4.19 или более ранней)

Важно: на сервер приложения категорически не рекомендуется устанавливать какие-либо приложения, отличные от Credit Registry.

1.5 Требования к оборудованию комплекса

Минимальные технические требования к оборудованию сервера:

- CPU: Intel Pentium 4 – 2,4 ГГц
- RAM: 2 ГБ
- HDD: объем для БД из оценки, что для хранения одного кредитного дела требуется 70КБ, для хранения кредитных отчетов по одному заявителю от трех БКИ – 30КБ.

На компьютере пользователя должны быть установлены:

- Браузер MS Internet Explorer 8 или выше, обеспечивающий доступ к web-серверу Credit Registry по протоколу http.

База данных (MS SQL Server / ORACLE/ PostgreSQL) и сервер приложений (Tomcat) могут быть разнесены и находиться на разных компьютерах. Tomcat по сути является web-сервером, приложение которого будет взаимодействовать с БД (MS SQL Server / ORACLE / PostgreSQL).

2 Установка Java Runtime Environment (JRE)

1. Скачайте и установите актуальную версию Java со следующей страницы:
<http://java.com/ru/download/manual.jsp>
2. Подтвердите значения параметров, предложенных по умолчанию. JRE должен быть установлен на тот же компьютер, куда будет устанавливаться Tomcat.
3. После установки JRE рекомендуется перезагрузить компьютер.

***Примечание:** Следует быть внимательным к ранее установленным версиям Java. Если на ПК установлена более ранняя версия Java, то рекомендуется ее удалить.*

3 Установка и настройка базы данных

Сервер БД используется сервером приложений для процедур хранения, извлечения и обработки необходимых данных. Набор необходимых данных формируется поступающими обработанными сервером приложений входящими данными. В качестве базы данных может использоваться MS SQL Server , ORACLE, PostgreSQL (см. п. 1.4 «Требования к общесистемному программному обеспечению»)

3.1 Установка MS SQL Server Express на Windows 7

Для случая минимальной установки на Windows 7 рекомендуется использовать MS SQL Server Express 2012 или выше.

Скачать MS SQL Server Express можно на сайте Microsoft:

2012: <https://www.microsoft.com/ru-RU/download/details.aspx?id=29062>

Разрядность ОС (32/64bit) не принципиальна. Рекомендуется скачивать и устанавливать файл вида SQLEXPADV_*.exe

При установке необходимо при выборе типа авторизации указать смешанный тип авторизации, а также указать (и запомнить!) пароль пользователя sa.

После установки необходимо зайти по следующему пути:

Меню Пуск - Все программы - Microsoft SQL Server - Средства настройки - Диспетчер конфигурации SQL Server:

Сетевая конфигурация SQL Server - Протоколы для SQLEXPRESS - TCP/IP - Свойства.

В открывшемся меню необходимо выставить: Включено - Да

На закладке IP-адреса для ВСЕХ адресов выставить: порт 1433, Активен - Да, Включено - Да.

После этого необходимо перезапустить службу SQL Server (это можно сделать из Диспетчера конфигурации SQL Server)

После этих операций необходимо создать БД на установленном MS SQL сервере.

Для этого в консоли SQL Server Management Studio выполните следующий набор команд:

```
CREATE LOGIN tutdf WITH PASSWORD='tutdf',CHECK_POLICY=OFF;  
CREATE DATABASE TUTDF COLLATE Cyrillic_General_CI_AS;  
GO  
USE TUTDF EXEC sp_changedbowner tutdf;
```

В результате будет создана база TUTDF, создан пользователь tutdf с паролем tutdf и назначен владельцем для базы TUTDF.

То же самое можно сделать из командной строки, для этого сохраните эти команды в файле (например, в: c:\create_db.sql) и выполните в командной строке на сервере, где установлен MS SQL, команду (пользователь Windows запускающий данную команду должен обладать ролью **sysadmin** на SQL сервере):

```
sqlcmd -S localhost -i c:\create_db.sql
```

(Соединение с именованным экземпляром с использованием проверки подлинности Windows:
sqlcmd -S <ComputerName>\<InstanceName>)

3.2 Установка MS SQL Server

Требования по версии MSSQL есть в разделе 1.4 «Требования к общесистемному программному обеспечению».

1. Дать наименование БД, например, tutdf.
2. Завести пользователя (например, TUTDF).
3. Присвоить пользователю права db_owner на эту базу.
4. Задать порт обращения к БД (по умолчанию 1433).
5. Указать кодировку Cyrillic_General_CI_AS.

3.3 Установка ORACLE

Требования по версии Oracle есть в разделе 1.4 «Требования к общесистемному программному обеспечению».

1. Дать наименование SID, например, tutdf (SID – это “System Identifier” базы данных).
2. Завести пользователя (например, TUTDF).
3. Присвоить пользователю права: connect и resource.
4. Задать порт обращения к БД (по умолчанию 1521).
5. Указать кодировку CL8MSWIN1251.

3.4 Установка PostgreSQL

Требования по версии PostgreSQL есть в разделе 1.4 «Требования к общесистемному программному обеспечению».

1. Дать наименование БД, например, tutdf.
2. Завести пользователя (например, tutdf).
3. Присвоить пользователю полные права GRANT ALL на эту базу.
4. Задать порт обращения к БД (по умолчанию 5432).
5. Указать кодировку WIN1251

3.5 Дополнительные утилиты для диагностики и настройки

При возникновении проблем с подключением к базе данных MS SQL могут понадобиться следующие программы:

Утилита telnet

Для проверки соединения по протоколу TCP/IP рекомендуется установить компоненту telnet, отключенную по умолчанию. Для ее установки перейдите в Панель управления, Программы и компоненты, Включение или отключение компонентов Windows, поставьте галочку - Клиент Telnet и нажмите кнопку ОК.

SQL Server Management Studio

Скачать средства управления можно по ссылке:

<https://msdn.microsoft.com/ru-ru/library/mt238290.aspx>

4 Установка Tomcat

1. Для установки Tomcat следует запустить apache-tomcat-7.0.x.exe и принять предложенные параметры установки;
2. Tomcat должен быть запущен как служба Windows;
3. Перед запуском Tomcat следует убедиться в том, что заведен пользователь с необходимыми правами для администрирования Tomcat в файле Tomcat\conf\tomcat-users.xml. Содержимое файла с минимальными настройками для запуска Tomcat:

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="admin-gui"/>
  <role rolename="manager-gui"/>
  <user username="admin" password="admin" roles=" admin-gui,manager-gui"/>
</tomcat-users>
```

Для развертывания war-файлов более 50MB измените в файле Tomcat\webapps\manager\WEB-INF\web.xml значение параметров:

- <max-file-size>52428800</max-file-size>
- <max-request-size>52428800</max-request-size>

на **209715200** (200MB)

4.1 Настройка средств диагностики при сбое Tomcat

В процессе работы приложения возможно возникновение ошибок сервера Tomcat. Ошибки в работе Tomcat могут происходить как из-за внутренних сбоев, так и быть следствием сбоев в Credit Registry. Для того чтобы диагностировать такие ошибки рекомендуется произвести следующие действия:

- Выполнить пункт меню Пуск/Программы/Apache Tomcat 7.0/Configure Tomcat
- Перейти на вкладку Java
- Добавить в поле Java Options следующие строки (в любое место):

```
-XX:+HeapDumpOnOutOfMemoryError  
-XX:HeapDumpPath=C:\Dump\  
-Dcom.sun.management.jmxremote.port=5670  
-Dcom.sun.management.jmxremote.ssl=false  
-Dcom.sun.management.jmxremote.authenticate=false
```

При копировании параметров из документации в поле Java Options убедитесь, что в конце строки отсутствует знак пробела.

C:\Dump\ – путь на файловой системе куда нужно произвести запись дампа Tomcat состояния системы на момент возникновения ошибки. Имея файл дампа Tomcat, заказчик или другое лицо эксплуатирующее приложение Credit Registry, может, связавшись с разработчиком Credit Registry, решить возникшую проблему быстрее, так как файл дампа предоставляет более подробную информацию о сбое. Хранение файлов дампа не является обязательным условием.

-Dcom.sun.management.jmxremote.port=5670 – здесь нужно вписать произвольный свободный порт. По этому порту будет доступен мониторинг нагрузки на Tomcat через jsconsole.

Внимание: Также время от времени рекомендуется производить очистку/архивацию папки logs, для предотвращения переполнения дискового пространства сервера. Для этого необходимо остановить работу Tomcat, так как в рабочем состоянии Tomcat не позволяет удалять свои файлы логирования.

После внесения изменений в настройки Tomcat, необходимо перезапустить службу Tomcat.

4.2 Настройка памяти Tomcat

Во избежание переполнения памяти Tomcat рекомендуется прописать следующие параметры:

В меню: Пуск/Программы/Apache Tomcat 7.0/Configure Tomcat в закладке Java:

- Initial memory pool – 256 MB
- Maximum memory pool – 768 MB
- В Java Options добавить строку (для Java 1.7):
-XX:MaxPermSize=256m

!Важно: в случае использования Java 8 параметр MaxPermSize игнорируется и его нужно плюсовать к Xmx (Maximum memory pool - 1024 MB)

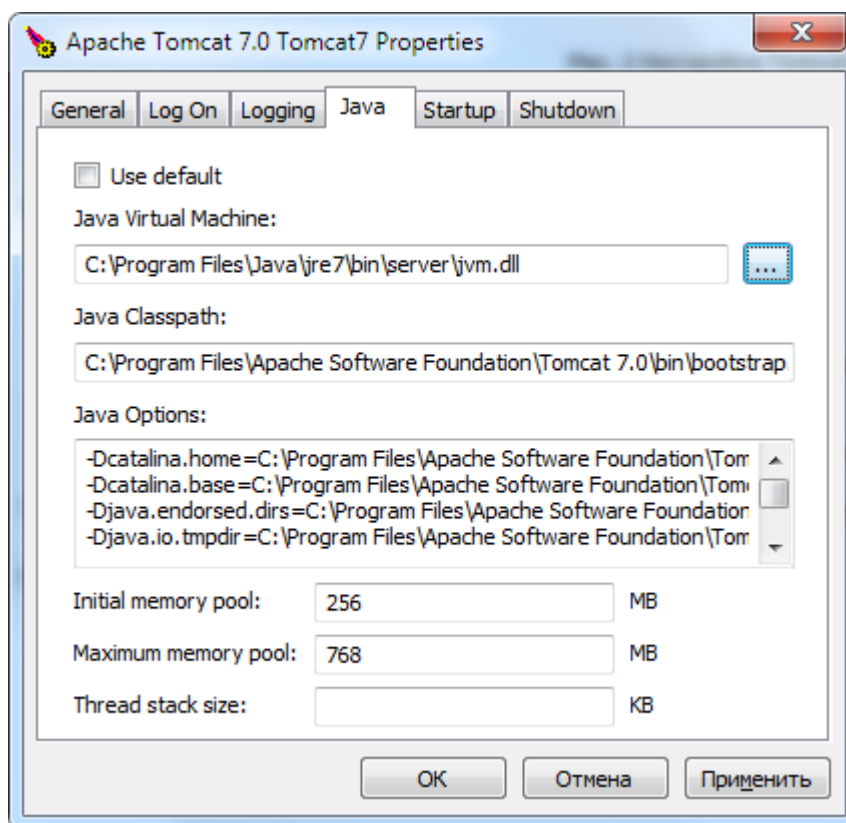


Рис. 1 Настройки Tomcat

4.3 Запуск Tomcat

Запустите сервер Tomcat.

Зайдите на корневую страницу Tomcat по адресу (например, <http://localhost:8080/>).

Управление настройками сервера происходит из консоли администрирования Tomcat Manager: перейдите по ссылке «Tomcat Manager» <http://localhost:8080/manager/html>, используя имя и пароль администратора Tomcat.

5 Соединение Tomcat с базой данных

Для развертывания на сервере приложение Credit Registry доступно в виде скомпилированного war-файла. Для развертывания приложения используется консоль администрирования Tomcat. Перед развертыванием приложения выполните следующие шаги:

5.1 Проверка корректности данных для соединения с БД

Перед настройкой Tomcat на соединение с БД мы рекомендуем проверить соединение с БД любым SQL-клиентом, например:

- для MS SQL Server – MS SQL Server Management Studio Express, Aqua Data Studio;
- для Oracle – Oracle SQL Developer, Aqua Data Studio, Quest Toad, DbVisualizer.
- Для PostgreSQL – PgAdmin, Aqua Data Studio.

Для соединения должны быть известны: тип БД, хост, порт, имя БД, логин, пароль.

Если с помощью какого-либо SQL-клиента подключиться к БД можно, то Credit Registry можно настраивать на эту БД.

5.2 Конфигурация соединения с базой данных

Настройки соединения с БД прописываются в файле Tomcat\conf\context.xml. (по умолчанию это C:\Program Files\Apache Software Foundation\Tomcat7.0\conf\context.xml)

Для того, чтобы настроить соединение с БД необходимо добавить в файл context.xml следующий фрагмент:

Для **MSSQL** (Tomcat 7.x):

Версия CreditRegistry < **7.15**:

```
<Resource name="jdbc/CRDb" auth="Container"
  type="javax.sql.DataSource"
  driverClassName="net.sourceforge.jtds.jdbc.Driver"
  validationQuery="select 1"
  url="jdbc:jtds:sqlserver://DATABASE_HOST_IP:PORT/DB_NAME"
  username="USERNAME"
  password="PASSWORD"
  maxActive="100"
  maxIdle="10"
  maxWait="-1"
  removeAbandoned="true"
  removeAbandonedTimeout="60"
  logAbandoned="true"/>
```

Версия CreditRegistry >= **7.15**:

```
<Resource name="jdbc/CRDb" auth="Container"
  type="javax.sql.DataSource"
  driverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver"
  validationQuery="select 1"
  url="jdbc:sqlserver://DATABASE_HOST_IP:PORT;databaseName=DB_NAME;
  sendStringParametersAsUnicode=false"
```

```
username="USERNAME"  
password="PASSWORD"  
maxActive="50"  
maxIdle="10"  
maxWait="-1"  
removeAbandoned="true"  
removeAbandonedTimeout="60"  
logAbandoned="true"  
</>
```

DATABASE_HOST_IP, **PORT**, **DB_NAME**, **USERNAME** и **PASSWORD** необходимо заменить на действительные значения.

При использовании Tomcat 8.x/9.x необходимо заменить параметры **maxActive** на **maxTotal**, **maxWait** на **maxWaitMillis**, **removeAbandoned** на **removeAbandonedOnBorrow**.

При использовании именованного экземпляра SQL Server (например, **INSTANCE1**) его можно указать следующим образом:

Для CreditRegistry < 7.15:

```
url="jdbc:jtds:sqlserver://DATABASE_HOST_IP/DB_NAME;instance=INSTANCE1"
```

Для CreditRegistry >= 7.15:

```
url="jdbc:sqlserver://DATABASE_HOST_IP;instanceName=INSTANCE1;databaseName=DB_NAME;sendStringParametersAsUnicode=false"
```

Для случая развертывания с настройками по умолчанию - **DATABASE_HOST_IP** = 127.0.0.1, **PORT** = 1433, **DB_NAME** = **USERNAME** = **PASSWORD** = tutdf.

Для **Oracle** (Tomcat 7.x):

```
<Resource name="jdbc/CRDb" auth="Container"  
type="javax.sql.DataSource"  
driverClassName="oracle.jdbc.OracleDriver"  
validationQuery="select 1 from dual"  
url="jdbc:oracle:thin:@DATABASE_HOST_IP:PORT:SID"  
username="USERNAME"  
password="PASSWORD"  
maxActive="100"  
maxIdle="10"  
maxWait="10000"  
removeAbandoned="true"  
removeAbandonedTimeout="60"  
logAbandoned="true"  
</>
```

DATABASE_HOST_IP, **PORT**, **SID**, **USERNAME** и **PASSWORD** необходимо заменить на действительные значения.

Для PostgreSQL:

```
<Resource name="jdbc/CRDb"
    auth="Container"
    type="javax.sql.DataSource"
    driverClassName="org.postgresql.Driver"
    validationQuery="select 1"
    url="jdbc:postgresql://DATABASE_HOST_IP/DB_NAME"
    username="USER_NAME" password="PASSWORD"
    maxTotal="100" maxIdle="10"
    maxWaitMillis="-1" removeAbandoned="true"
    removeAbandonedOnBorrow="true"
removeAbandonedTimeout="60"
    logAbandoned="true"
/>
```

DATABASE_HOST_IP, DB_NAME, USER_NAME и PASSWORD необходимо заменить на действительные значения.

При использовании Tomcat 8.x/9.x необходимо заменить параметры maxActive на maxTotal, maxWait на maxWaitMillis, removeAbandoned на removeAbandonedOnBorrow.

Также в общие библиотеки Tomcat (Tomcat\lib\) необходимо подложить драйвер соединения с БД:

для Oracle* <http://creditregistry.ru/download/ojdbc7.jar>

Примечание*: рекомендуем использовать актуальный драйвер с сайта Oracle (<http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html>).

для MSSQL:

для версии CreditRegistry < 7.15: <http://creditregistry.ru/download/jtds-1.3.1.jar>

для версии CreditRegistry >= 7.15: <http://creditregistry.ru/download/sqljdbc41.jar>

для версий CreditRegistry >=2022.1: <http://creditregistry.ru/download/mssql-jdbc-8.2.1.jre8.jar>

Для PostgreSQL: <http://www.creditregistry.ru/download/postgresql-42.3.3.jar>

После изменений в файле context.xml необходимо перезапустить сервис Tomcat.

5.2.1 Дополнительные настройки

Значение параметра **maxActive, maxTotal (MSSQL/Oracle/PostgreSQL)** может отличаться от типового, это зависит от требований к производительности приложения, для типовой установки рекомендуется указать значение: 50 (MS SQL Server / Oracle/ PostgreSQL).

Неверно настроенный размер пула соединений с базой данных может приводить к значительному ухудшению пропускной способности и производительности системы.

Рекомендуемая формула для оценки размера пула:

Размер пула = (Максимальное кол-во параллельных вызовов коннекторов + 1) X 2 +
+ (Кол-во активных пользователей в системе) +
+ (Максимальное кол-во параллельных импортов и экспортов) X 3

Размер пула рекомендуется всегда задавать через настройки в файле **context.xml**.

Внимание: После внесения изменений в файл context.xml необходимо перезапустить сервис Tomcat.

6 Развертывание приложения Credit Registry на Tomcat

6.1 Установка

Внимание: Рекомендуется производить резервное копирование Базы Данных (БД), используемой системой Credit Registry перед каждой установкой новой версии. Инструкция по обновлению приложения приведена в «ПРИЛОЖЕНИЕ С. Установка новых версий приложения».

В форме “WAR file to deploy” укажите путь к файлу credit_registry.war из дистрибутива.

Обычно, war-файл предоставляется по ссылке вида: http://creditregistry.ru/vX.YY.ZZ/credit_registry.war.zip, где X.YY.ZZ – номер версии CreditRegistry.

Номер последней рекомендуемой версии необходимо уточнять у техподдержки МТЦ.

После того, как файл выбран, нажмите кнопку “Deploy”. После установки в списке web-приложений появится “Credit Registry” (показано на рисунке внизу). Убедиться в том, что приложение установлено и работает, можно по появившемуся в колонке Applications/Path названию приложения и статус Running = True.

Manager				
List Applications	HTML Manager Help	Manager Help	Server Status	

Applications				
Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/credit_registry	Credit Registry	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Deploy
Deploy directory or WAR file located on server
Context Path (optional): <input type="text"/>
XML Configuration file URL: <input type="text"/>
WAR or Directory URL: <input type="text"/>
<input type="button" value="Deploy"/>

WAR file to deploy
Select WAR file to upload <input type="text"/> <input type="button" value="Browse..."/>

Рис. 2 Установка Credit Registry

6.2 Важные рекомендации

Для корректной работы приложения Credit Registry, а также для предотвращения нештатных ситуаций, связанных с потерей данных, настоятельно рекомендуется всегда следовать следующим рекомендациям:

- 1) осуществлять перезапуск сервиса Apache Tomcat после установки новой версии Credit Registry;
- 2) осуществлять регулярную очистку директорий **temp** и **work**, находящихся в директории с установленным Apache Tomcat сервером - ("*C:\Program Files\Apache Software Foundation\Tomcat7\temp*" и "*C:\Program Files\Apache Software Foundation\Tomcat7\work*");
- 3) осуществлять регулярную очистку директории журналов **logs**, находящейся в директории с установленным Apache Tomcat сервером - "*C:\Program Files\Apache Software Foundation\Tomcat7\logs*";
- 4) использовать сжатие для NTFS для директории журналов **logs**, находящейся в директории с установленным Apache Tomcat сервером - "*C:\Program Files\Apache Software Foundation\Tomcat7\logs*";
- 5) производить резервное копирование базы данных, используемой Credit Registry перед установкой новой версии.

6.3 Запуск приложения

Зайдите в приложение Credit Registry (http://localhost:8080/credit_registry), вызвав его из Web консоли Tomcat из вкладки Applications. Первый вход в приложение может длиться некоторое время, так как будут заполняться справочники системы. При запуске приложения будет заведена учетная запись администратора Credit Registry (пользователь: admin, пароль: admin).

7 Настройка соединения с НБКИ

В соответствии с техническим регламентом НБКИ для передачи запросов на получение кредитных историй в НБКИ требуется наличие защищенного канала, по которому протокол прикладной программы будет передавать и получать данные. Для обеспечения защищенного соединения используются сертификаты подлинности и программный продукт SSLGate.

Программный продукт SSLGate предназначен для туннелирования http-трафика, шифрования его в соответствии с имеющимся сертификатом и передачи на сервер получателя. **SSLGate** – программный продукт для организации защищённого удалённого доступа на уровне SSL-канала. Для работы SSL требуется, чтобы на сервере имелся SSL-сертификат. При использовании SSL-сертификата создаётся защищённое соединение между клиентом и сервером. SSL использует шифрование с открытым ключом для подтверждения подлинности отправителя и получателя.

7.1 Настройка шлюза поддержки защищенного соединения для Credit Registry (НБКИ)

Для настройки запросов в НБКИ необходимо:

1. Войти в систему с правами администратора (может использоваться как машина с Tomcat+CRE, так и отдельный сервер).
2. Установить на компьютер КриптоПро CSP 3.6/3.9/4.0
3. Установить SSLGate. Дистрибутив можно скачать по ссылке:

<http://creditregistry.ru/download/SSLgateNet4.17.zip>

Для связи с НБКИ используются корневые сертификаты УЦ КРИПТО-ПРО, которые должны быть установлены в доверенные корневые центры сертификации в локальное хранилище компьютера.

Актуальные сертификаты УЦ КРИПТО-ПРО доступны по адресу <http://cpca20.cryptopro.ru/cacer.p7b>

4. Настроить коннектор (см. ниже).
5. Добавить права на коннектор в ролях тех пользователей, которые будут отправлять запросы в НБКИ.

7.2 Настройка коннектора НБКИ в Credit Registry

Для связи с НБКИ необходимо на машине с SSLGate открыть доступ к серверу icrs.nbki.ru по порту 443 напрямую. Если доступ открывается через прокси-сервер, необходимо следовать инструкции «Настройка прокси-соединения для связи сервера Credit Registry с БКИ» в данной документации.

Примечание. Для доступа по http (т.е. для тестового доступа) порт необходимо открывать с сервера Tomcat.

Прежде чем производить настройку параметров доступа к НБКИ рекомендуется ознакомиться с документом «Руководство пользователя Credit Registry».

Настройку системы Credit Registry должен проводить пользователь (администратор), у которого установлены права на:

- Редактирование пользователей и прав;
- Редактирование параметров коннектора;
- Редактирование справочник сертификатов.

После добавления нового коннектора устанавливаются следующие параметры:

Редактирование профиля коннектора

Коннектор: **НБКИ**

Название профиля: НБКИ B2B

Описание профиля: НБКИ B2B

Приоритет профиля: 100

Код участника: 0001ZZ000000

Имя: 0001ZZ000003

Пароль: ••••••••

Запретить в пользовательском интерфейсе выбор сервисов

Сервисы НБКИ

Адрес основного сервиса: <https://icrs.nbki.ru/products/B2BRequestServlet>

Адрес FICO сервиса: <https://icrs.nbki.ru/score>

Адрес FICO2 сервиса: <https://icrs.nbki.ru/score2>

Адрес Fico Expansion Score сервиса: <https://icrs.nbki.ru/expansionScore>

Разрешить запрос Fico Expansion Score

Адрес сервиса "Истории Историй": <https://icrs.nbki.ru/ChhService/B2BRequestServlet>

Адрес сервиса "Анализ социальных сетей": <https://icrs.nbki.ru/sna>

Адрес FICO Fraud сервиса: <https://icrs.nbki.ru/fraudScore>

Адрес сервиса "Истории Историй" + FICO: https://icrs.nbki.ru/chhs_score2

Сертификат Fico Expansion и Fico Fraud Score: Тестовый пользователь 2014

Использование сервисов по умолчанию: Только отчет НБКИ

Универсальный сервис

Адрес универсального сервиса: <https://icrs.nbki.ru/universalService>

Доступные сервисы	По умолчанию
<input checked="" type="checkbox"/> Сервис "Истории историй"	<input type="checkbox"/>
<input checked="" type="checkbox"/> Сервис FICO2	<input type="checkbox"/>
<input checked="" type="checkbox"/> Сервис FICO3	<input type="checkbox"/>
<input checked="" type="checkbox"/> Сервис FICO FRAUD	<input type="checkbox"/>
<input checked="" type="checkbox"/> Сервис "Анализ социальных связей"	<input type="checkbox"/>
<input checked="" type="checkbox"/> Кредитный отчет с информационной частью	<input type="checkbox"/>
<input checked="" type="checkbox"/> Только информационная часть	<input type="checkbox"/>
<input checked="" type="checkbox"/> Сервис "Double Data (SA)"	<input type="checkbox"/>
<input checked="" type="checkbox"/> Сервис "Double Data (SL)"	<input type="checkbox"/>

Рис. 3 Настройки профиля коннектора НБКИ

Настройки кэша

Глубина используемого кэша:

Есть кредитная история	<input type="text"/>
Только запросы	<input type="text"/>
Нет данных	<input type="text"/>
Ошибка	<input type="text"/>

Кэшировать несодержательные ответы

Установить запрет на отключение кэша

Настройки соединения с сервисом

Время ожидания ответа сервиса: сек

Максимальное количество соединений:

Максимальное время ожидания в очереди: сек

Максимальное время установления SSL-соединения: сек

Расширенные настройки коннектора

Максимальное количество переповторов:

Интервал между переповторами: сек

Список ошибок, при которых выполнять переповтор

- ошибка формирования ЭЦП для запросов (SSLGate)
- таймаут формирования ЭЦП для запросов (SSLGate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSLGate
- ошибка/таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 4 Настройки профиля коннектора НБКИ

Параметр	Рекомендации
Коннектор	Содержит название коннектора, автоматически заполняется системой
Название профиля	Содержит название профиля коннектора, заполняется пользователем
Описание профиля	Содержит описание профиля коннектора
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большшему числу соответствует больший приоритет
Код участника	Выдают менеджеры НБКИ (например: 0101BV000000)

Имя	Имя пользователя для выполнения запросов, выдают менеджеры НБКИ (например: 0101BV000001)
Пароль	Пароль пользователя для выполнения запросов, выдают менеджеры НБКИ
Запретить в пользовательском интерфейсе выбор сервисов	Установленная галка запрещает пользователям выполнять запросы со скорингом (через UI)
Сервисы НБКИ	
Адрес основного сервиса	Для демо-доступа http://icrs.demo.nbki.ru/products/B2BRequestServlet или https://icrs.demo.nbki.ru/products/B2BRequestServlet Для «боевого» доступа https://icrs.nbki.ru/products/B2BRequestServlet
Адрес FICO сервиса	Для тестового доступа http://icrs.demo.nbki.ru/score или https://icrs.demo.nbki.ru/score Для «боевого» доступа https://icrs.nbki.ru/score
Адрес FICO2 сервиса	Для тестового доступа (те же адреса, что и для fico) http://icrs.demo.nbki.ru/score или https://icrs.demo.nbki.ru/score Для «боевого» доступа https://icrs.nbki.ru/score2
Адрес Fico Expansion Score сервиса	Для тестового доступа https://icrs.demo.nbki.ru/expansionScore или http://icrs.demo.nbki.ru/expansionScore Для «боевого» доступа https://icrs.nbki.ru/expansionScore Примечание. Для работы с Expansion Score необходимо поставить в настройках коннектора галочку "Разрешен запрос Fico Expansion Score".
Разрешить запрос Fico Expansion Score (флаг)	Установленный флаг разрешает запрашивать информацию Fico Expansion Score
Адрес сервиса «Истории Историй»	https://icrs.nbki.ru/ChhService/B2BRequestServlet На стороне НБКИ тестового сервиса истории историй нет.
Адрес сервиса «Анализ социальных сетей»	Для промышленного доступа https://icrs.nbki.ru/sna
Адрес FICO Fraud сервиса	Для «боевого» доступа: https://icrs.nbki.ru/fraudScore Реализация тестового режима отсутствует.
Адрес сервиса «Истории Историй» + FICO	Для «боевого» доступа: https://icrs.nbki.ru/chhs_score2 Реализация тестового режима отсутствует.

Номер сертификата Fico Expansion и Fico Fraud Score	Личный сертификат. Получается в НБКИ. Если Expansion score и Fico Fraud Score не используются, получение сертификата необязательно. Можно использовать тот же сертификат, что и для запросов ФМС и ГИБДД.
Использование сервисов по умолчанию	<ul style="list-style-type: none"> • Только отчет НБКИ • Отчет со скорингом FICO (если адрес сервиса FICO не будет указан, то будет использован адрес сервиса FICO2) • Отчет со скорингом FICO2 • Отчет с «Историей историй» • Отчет с анализом социальных связей • Отчет со скорингом FICO Fraud • Отчет с «Историей историй» + FICO
Универсальный сервис	
Адрес Универсального сервиса	Содержит адрес подключения к Универсальному сервису НБКИ. Адрес точки входа: https://icrs.nbki.ru/universalService
Доступные сервисы: <ul style="list-style-type: none"> • Сервис «Истории историй» • Сервис FICO2 • Сервис FICO3 • Сервис FICO FRAUD • Сервис «Анализ социальных связей» • Кредитный отчет с информационной частью • Только информационная часть • Сервис "Double Data (SA)" • Сервис "Double Data (SL)" 	Набор флагов, указывающий доступные сервисы, к которым будет обращаться CRE при отправке запроса с помощью Универсального сервиса НБКИ. Флаги «включить по умолчанию» определяют доступные для пользователя сервисы (указываются администратором системы).
Настройки кэша	
Глубина используемого кэша Есть кредитная история Только запросы Нет данных Ошибка	Задается в днях. Перед запросом в бюро Credit Registry просматривает историю запросов. Если такой же запрос повторялся, то определяется его тип (есть КИ, только запросы, нет данных, ошибка) и выполняется проверка, попадает ли он в заданный интервал кэширования. Если попадает, то ответ возвращается из кэша, иначе выполняется запрос в бюро. Если значение в поле «Есть кредитная история», «Только запросы», «Нет данных» или «Ошибка» не задано, то используется значение из поля «Глубина используемого кэша». Использование кэша позволяет экономить на часто повторяющихся запросах. <u>Пример работы с кэшем (для всех коннекторов)</u> Если в параметре «глубина использования кэша» в профиле какого-либо коннектора указать значение «1» (cache_use=1) и выполнить запрос 08.05.2014 в 13:00, то поиск ответов в кэше

	<p>будет выполняться до 07.05.2014 00:00. Если же указать значение «2» и выполнить запрос также в 08.05.2014 в 13:00, то данные в кэше будут проверяться до 06.05.2014 00:00. Таким образом, указываемое в параметре «глубина использования кэша» значение – это количество полных календарных суток, прошедшее до момента выполнения запроса.</p> <p>Как правило, в параметре указываются значения от 1 до 5 дней. Пользователь может указывать и БОльшие значения, но при этом необходимо учитывать, что из кэша могут вернуться достаточно давние, и, возможно, уже неактуальные данные.</p>
Кэшировать несодержательные ответы	<p>В истории запросов в любом случае сохраняются все ответы. Но если ответ был несодержательным (бюро ответило ошибкой), то такой запрос вернется из кэша только в случае, когда галочка стоит. Обычно эта опция отключена.</p>
Установить запрет на использование кэша	<p>Установленный флаг запрещает пользователям отключать кэш</p>
Настройки соединения с сервисом	
Время ожидания ответа от сервиса	<p>Время ожидания ответа от сервиса после установления соединения. Рекомендуемое значение: 60 сек.</p>
Максимальное количество соединений	<p>Максимальное количество одновременных соединений с сервисом. Рекомендуемое значение: 20.</p>
Максимальное время ожидания в очереди	<p>Максимальное время ожидания в очереди для соединений, превышающих максимальное количество одновременных соединений с сервисом. Рекомендуемое значение: 30 сек.</p>
Максимальное время установления SSL соединения	<p>Максимальное время установления SSL соединения с сервисом. Рекомендуемое значение: 30 сек.</p>
Расширенные настройки коннектора	
Максимальное количество переповторов	<p>Указывается максимальное количество переповторов, которое будет производится системой</p>
Интервал между переповторами	<p>Интервал между переповторами в секундах</p>
Список ошибок, при которых выполнять переповтор	<p>Ошибка формирования ЭЦП для запросов (SSL Gate) Таймаут формирования ЭЦП для запросов (SSL Gate) Таймаут ожидания в очереди коннектора Ошибки соединений с SSLGate Ошибка/таймаут соединений с БКИ Таймаут ответа БКИ или внешнего источника Прочие сетевые ошибки Ошибка БКИ или внешнего источника в прикладном протоколе</p>

Обратите внимание, что для обеспечения работы с НБКИ, пользователям необходимо предоставлять доступ к коннектору через роль. То есть в свойствах роли (закладка «Администрирование» - таблица «Роли» - форма редактирования) в блоке «Доступ к коннекторам» необходимо установить флаг «НБКИ В2В».

Дополнение:

После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение G. Типичные ошибки настройки коннекторов** (стр. 132).

Замечание: если в «Администрирование» – «Параметры» – «Остальные настройки» установить галку «Расширенные настройки коннектора», то у коннектора появятся дополнительные настройки для выполнения повторных запросов в БКИ (при возникновении каких-либо технических ошибок):

Остальные настройки

Глубина секции **current** (StatusMonitor) по умолчанию 30 циклов (статистика за 5 мин)

Архивировать запросы-ответы коннекторов старше дней

Директория загрузки ответов НБКИ

Логотип в заголовке

Режим совместимости WSDL

Расширенные настройки коннектора ⚠

Отключить расширенную валидацию по справочникам

Активировать справочник программ кредитования

Проверять описания пользователей на уникальность

Рис. 5 Блок параметров «Остальные настройки»

Расширенные настройки коннектора

Максимальное количество переповторов

Интервал между переповторами сек

Список ошибок, при которых выполнять переповтор

- ошибка формирования ЭЦП для запросов (SSLGate)
- таймаут формирования ЭЦП для запросов (SSLGate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSLGate
- ошибка/таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 6 Блок параметров «Расширенные настройки коннектора»

7.3 Настройка параметров коннектора ФМС

Для связи с НБКИ необходимо на машине с SSLGate открыть доступ к серверу icrs.nbki.ru по порту 443 напрямую. Если доступ открывается через прокси-сервер, необходимо следовать инструкции «Настройка прокси-соединения для связи сервера Credit Registry с БКИ» в данной документации.

Примечание. Для доступа по http (т.е. для тестового доступа) порт необходимо открывать с сервера с Tomcat.

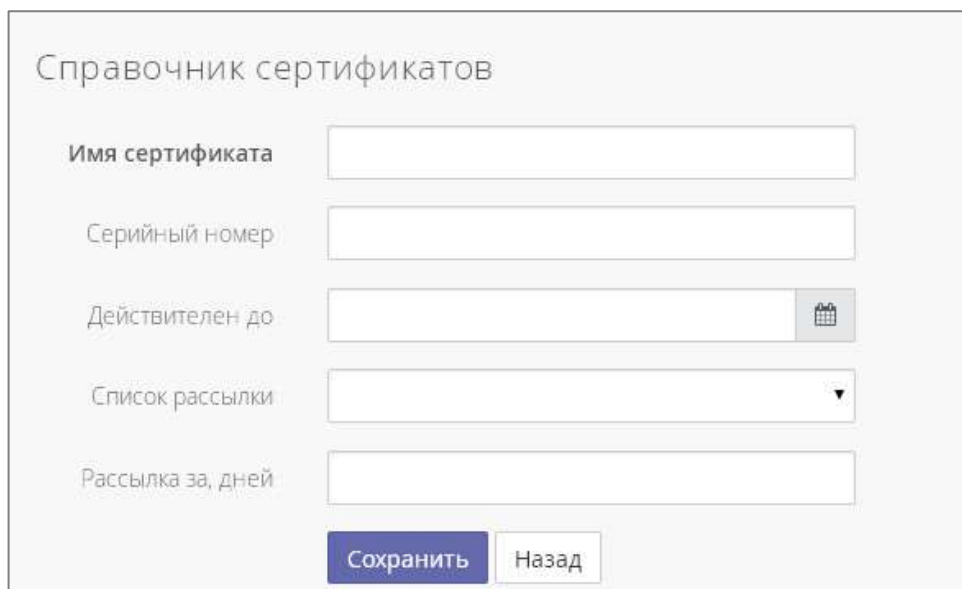
Простой и расширенный отчеты отличаются тем, что в ответ на простой запрос в ответе возвращается только последнее состояние (один тэг record), а на расширенный возвращается вся история изменений, т.е. тэгов record может быть несколько.

Прежде чем производить настройку параметров доступа к указанным сервисам рекомендуется ознакомиться с документом «Руководство пользователя Credit Registry».

Примечание: Если у вас уже есть настроенный и работающий коннектор (для одного из сервисов ФМС, ГИБДД, ТСЗ или БРС), и вам нужно настроить другой коннектор из этого списка, то код участника, логин, пароль и сертификат можно скопировать из уже настроенного.

Для начала работы с сервисом ФМС, необходимо выполнить такие действия:


1. На машине с SSLGate установить личный сертификат в сертификаты локального компьютера, следуя инструкции Приложения А. (Личный и корневой сертификаты получают в НБКИ).
2. Войти в систему Credit Registry и добавить серийный номер сертификата в «Справочник сертификатов» (см. «Руководство пользователя Credit Registry»).



Справочник сертификатов

Имя сертификата

Серийный номер

Действителен до 

Список рассылки ▼

Рассылка за, дней

Рис. 7 Добавление сертификата в справочник сертификатов

На закладке «Администрирование» найти раздел «Сертификаты» и воспользоваться кнопкой «добавить» в правом верхнем углу таблицы. Впоследствии введенный номер сертификата необходимо указывать в настройках коннектора.

3. Настроить параметры коннекторов соответствующих сервисов.

После добавления нового коннектора для сервиса НБКИ ФМС устанавливаются следующие параметры:

Добавление профиля коннектора

Коннектор:

Название профиля:

Описание профиля:

Приоритет профиля:

Адрес сервиса:

Код участника:

Имя:

Пароль:

Сертификат:

Настройки кэша

Глубина используемого кэша:

Кэшировать несодержательные ответы

Установить запрет на отключение кэша

Настройки соединения с сервисом

Время ожидания ответа сервиса: сек

Максимальное количество соединений:

Максимальное время ожидания в очереди: сек

Максимальное время формирования ЭЦП: сек

Максимальное время установления SSL соединения: сек

Рис. 8 Настройки профиля коннектора ФМС

Параметр	Рекомендации
Коннектор	Содержит название коннектора, автоматически заполняется системой
Название профиля	Содержит название профиля коннектора, заполняется пользователем
Описания профиля	Содержит описание профиля коннектора
Приоритет профиля	Число, должно быть уникальным для каждого профиля. Большем числу соответствует больший приоритет.
Адрес сервиса	«Боевой» адрес сервиса: https://icrs.nbki.ru/fms Для тестирования и отладки можно использовать адрес: http://fms.demo.nbki.ru:8080/FmsService/fms

Параметр	Рекомендации
Код участника, Имя и Пароль	Информация предоставляется менеджерами НБКИ. Код участника НБКИ имеет последние шесть нулей, имя аналогично коду участника НБКИ, но последние шесть цифр пять нулей и единичка.
Сертификат	Указывается сертификат из выпадающего списка (чтобы сертификат был в списке его необходимо добавить в разделе «Сертификаты» на странице «Администрирование»)
Настройки кэша	
Глубина используемого кэша	Задается в днях. Перед запросом в бюро Credit Registry просматривает историю запросов. Если такой же запрос повторялся на протяжении последних <глубина кэша> дней, то ответ вернется из кэша.
Кэшировать несодержательные ответы	В истории запросов, в любом случае, сохраняются все ответы. Но если ответ был несодержательным (бюро ответило ошибкой), то такой запрос вернется из кэша только в случае, когда галочка стоит. Обычно эта опция отключена.
Установит запрет на отключение кэша	Установленный флаг запрещает отключать кэш
Настройки соединения с сервисом	
Время ожидания ответа сервиса	Рекомендуемое значение: 330 сек.
Максимальное количество соединений	Рекомендуемое значение: 20.
Максимальное время ожидания в очереди	Рекомендуемое значение: 30 сек.
Максимальное время формирования ЭЦП	Рекомендуемое значение: 30 сек.
Максимальное время установления SSL соединения	Рекомендуемое значение: 30 сек.

4. Добавить права на коннектор в ролях тех пользователей, которые будут отправлять запросы, соответствующие сервисы.
5. Зайти на закладку ФМС, сделать запрос.

Дополнение:

Список типичных ошибок настройки коннекторов приведен в данной документации:

Приложение G. Типичные ошибки настройки коннекторов (стр. 132).

7.4 Настройки параметров коннектора ГИБДД

Для связи с НБКИ необходимо на машине с SSLGate открыть доступ к серверу icrs.nbki.ru по порту 443 напрямую. Если доступ открывается через прокси-сервер, необходимо следовать инструкции «Настройка прокси-соединения для связи сервера Credit Registry с БКИ» в данной документации.

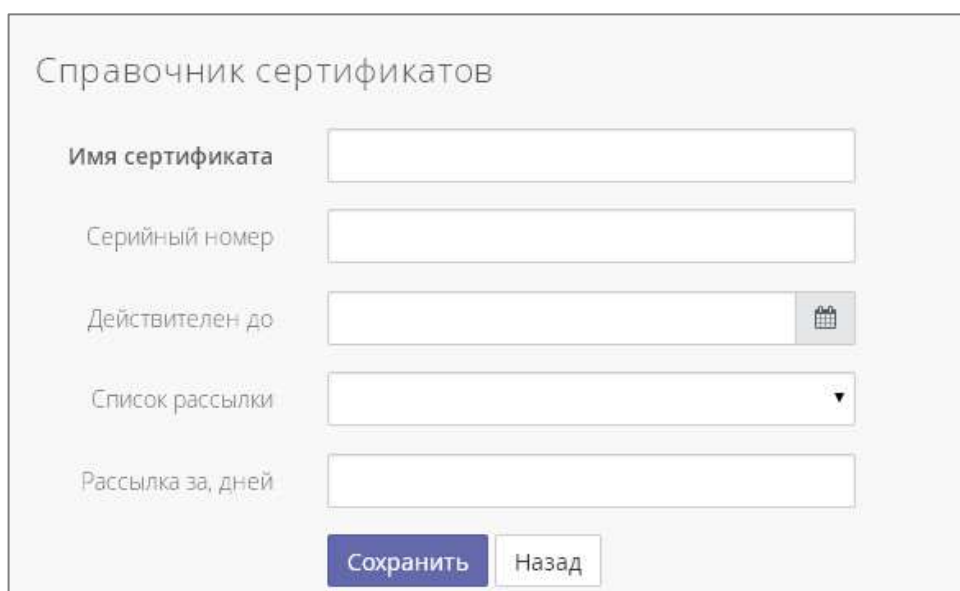
Примечание. Для доступа по http (т.е. для тестового доступа) порт необходимо открывать с сервера с Tomcat.

Прежде чем производить настройку параметров доступа к указанным сервисам рекомендуется ознакомиться с документом «Руководство пользователя Credit Registry».

Примечание: Если у вас уже есть настроенный и работающий коннектор (для одного из сервисов ФМС, ФМС2, ГИБДД, ТСЗ или БРС), и вам нужно настроить другой коннектор из этого списка, то код участника, логин, пароль и сертификат можно скопировать из уже настроенного.

Для начала работы с сервисом НБКИ ГИБДД, необходимо выполнить такие действия:


1. На машине с SSLGate установить личный сертификат в сертификаты локального компьютера, следуя инструкции Приложения А. (Личный и корневой сертификаты получают в НБКИ).
2. Войти в систему Credit Registry и добавить серийный номер сертификата в «Справочник сертификатов» (см. «Руководство пользователя Credit Registry»).



Справочник сертификатов

Имя сертификата

Серийный номер

Действителен до 

Список рассылки ▼

Рассылка за, дней

Рис. 9 Добавление сертификата в справочник сертификатов

На закладке «Администрирование» найти раздел «Сертификаты» и воспользоваться ссылкой «добавить» в правом верхнем углу таблицы. Впоследствии введенный номер сертификата необходимо указывать в настройках коннектора.

3. Настроить параметры коннектора.

После добавления нового коннектора для сервиса НБКИ ГИБДД устанавливаются следующие параметры:

Параметр	Рекомендации
Коннектор	Содержит название коннектора, автоматически заполняется системой
Название профиля	Содержит название профиля коннектора, заполняется пользователем
Описание профиля	Содержит описание профиля коннектора
Приоритет профиля	Число, должно быть уникальным для каждого профиля. Большшему числу соответствует больший приоритет.
Адрес сервиса	«Боевой» адрес сервиса: https://icrs.nbki.ru/gibdd Для тестирования и отладки можно использовать адрес: http://gibdd.demo.nbki.ru:8080/GibddService/gibdd
Код участника, Имя и Пароль	Информация предоставляется менеджерами НБКИ. Код участника НБКИ имеет последние шесть нулей, имя аналогично коду участника НБКИ, но последние шесть цифр пять нулей и единичка.
Сертификат	Указывается сертификат из выпадающего списка (чтобы сертификат был в списке его необходимо добавить в разделе «Сертификаты» на странице «Администрирование»)
Строгая проверка обязательности полей формы	Флаг активирует проверку обязательности заполнения полей формы
Настройки кэша	
Глубина используемого кэша	Задается в днях. Перед запросом в бюро Credit Registry просматривает историю запросов. Если такой же запрос повторялся на протяжении последних <глубина кэша> дней, то ответ вернется из кэша.
Установить запрет на отключение кэша	Если галочка выставлена, пользователи не смогут делать запросы без использования кэша
Настройки соединения с сервисом	
Время ожидания ответа от БКИ	Рекомендуемое значение: 930 сек. Примечание: 930 сек = 15 мин + 30 сек = (Таймаут ожидания ответа ГИБДД, установленный на стороне НБКИ) + 30 сек.
Максимальное количество соединений	Рекомендуемое значение: 20.
Максимальное время ожидания в очереди	Рекомендуемое значение: 30 сек.
Максимальное время формирования ЭЦП	Рекомендуемое значение: 30 сек.

Максимальное время установления SSL соединения	Рекомендуемое значение: 30 сек.
--	---------------------------------

Добавление профиля коннектора

Коннектор:

Название профиля:

Описание профиля:

Приоритет профиля:

Адрес сервиса:

Код участника:

Имя:

Пароль:

Сертификат:

Строгая проверка обязательности полей формы

Настройки кэша

Глубина используемого кэша:

Установить запрет на отключение кэша

Настройки соединения с сервисом

Время ожидания ответа сервиса: сек

Максимальное количество соединений:

Максимальное время ожидания в очереди: сек

Максимальное время формирования ЭЦП: сек

Максимальное время установления SSL соединения: сек

Рис. 10 Добавление профиля коннектора НБКИ ГИБДД

- Добавить права на коннектор в ролях тех пользователей, которые будут отправлять запросы, соответствующие сервисы.

НБКИ ГИБДД НБКИ ГИБДД

Рис. 11 Флаг коннектора НБКИ ГИБДД в списке прав роли

Дополнение:

После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение Г. Типичные ошибки настройки коннекторов** (стр. 132).

7.5 Настройки параметров коннектора ТСЗ

Для связи с НБКИ необходимо на машине с SSLGate открыть доступ к серверу icrs.nbki.ru по порту 443 напрямую. Если доступ открывается через прокси-сервер, необходимо следовать инструкции «Настройка прокси-соединения для связи сервера Credit Registry с БКИ» в данной документации.

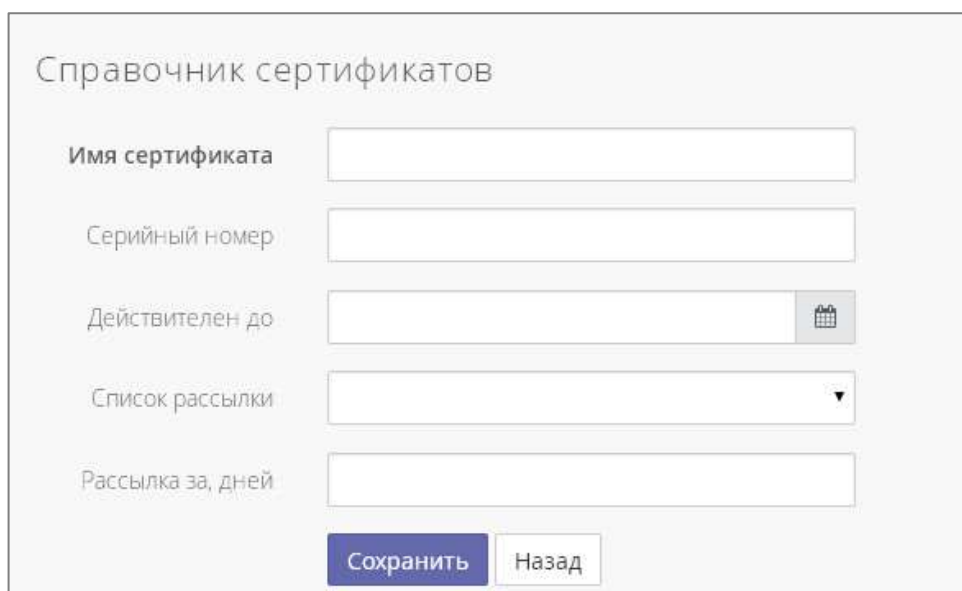
Примечание. Для доступа по http (т.е. для тестового доступа) порт необходимо открывать с сервера с Tomcat.

Прежде чем производить настройку параметров доступа к сервису НБКИ ТСЗ рекомендуется ознакомиться с документом «Руководство пользователя Credit Registry».

Примечание: Если у вас уже есть настроенный и работающий коннектор (для одного из сервисов ФМС, ФМС2, ГИБДД, ТСЗ или БРС), и вам нужно настроить другой коннектор из этого списка, то код участника, логин, пароль и сертификат можно скопировать из уже настроенного.

Необходимо выполнить такие действия:


1. На машине с SSLGate установить личный сертификат в сертификаты локального компьютера, следуя инструкции Приложения А. (Личный и корневой сертификаты получают в НБКИ).
2. Войти в систему Credit Registry и добавить серийный номер сертификата в [«Справочник сертификатов»](#) (см. «Руководство пользователя Credit Registry»).



Справочник сертификатов

Имя сертификата

Серийный номер

Действителен до 

Список рассылки

Рассылка за, дней

Рис. 12 Добавление сертификата в справочник сертификатов

На закладке [«Администрирование»](#) найти раздел [«Сертификаты»](#) и воспользоваться ссылкой **«добавить»** в правом верхнем углу таблицы. Впоследствии введенный номер сертификата необходимо указывать в настройках коннектора.

3. Настроить параметры коннектора.

После добавления нового коннектора для сервиса НБКИ ТСЗ (залоговые транспортные средства) устанавливаются следующие параметры:

Добавление профиля коннектора

Коннектор: НБКИ ТСЗ

Название профиля: НБКИ ТСЗ

Описание профиля: НБКИ ТСЗ

Приоритет профиля: 123

Адрес сервиса: <https://icrs.nbki.ru/collatauto>

Код участника: 000122000000

Имя: 000122000003

Пароль: *****

Сертификат: Оператор НБКИ - 2014

Настройки соединения с сервисом

Время ожидания ответа сервиса: сек

Максимальное количество соединений:

Максимальное время ожидания в очереди: сек

Максимальное время формирования ЭЦП: сек

Максимальное время установления SSL-соединения: сек

Сохранить Назад

Рис. 13 Добавление профиля коннектора НБКИ ТСЗ

Параметр	Рекомендации
Коннектор	Содержит название коннектора, автоматически заполняется системой
Название профиля	Содержит название профиля коннектора, заполняется пользователем
Описание профиля	Содержит описание профиля коннектора
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большемому числу соответствует больший приоритет.
Адрес сервиса	«Боевой» адрес сервиса: https://icrs.nbki.ru/collatauto Для тестирования и отладки можно использовать адрес: http://collatauto.demo.nbki.ru:8080/CollatAuto/collatauto
Код участника, Имя и Пароль	Информация предоставляется менеджерами НБКИ. Код участника НБКИ имеет последние шесть нулей, имя аналогично коду участника НБКИ, но последние шесть цифр пять нулей и единичка.
Сертификат	Указывается сертификат из выпадающего списка (чтобы сертификат был в списке его необходимо добавить в разделе «Сертификаты» на странице «Администрирование»)
Настройки соединения с сервисом	

Время ожидания ответа сервиса	Рекомендуемое значение: 60 с.
Максимальное количество соединений	Рекомендуемое значение: 20
Максимальное время ожидания в очереди	Рекомендуемое значение: 30 с.
Максимальное время формирования ЭЦП	рекомендуемое значение: 30 с.
Максимальное время установления SSL соединения	Рекомендуемое значение: 30 с.

4. Добавить права на коннектор в ролях тех пользователей, которые будут отправлять запросы, соответствующие сервисы.



Рис. 14 Флаг коннектора НБКИ ТСЗ в списке прав роли

Дополнение:

После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение Г. Типичные ошибки настройки коннекторов** (стр. 132).

7.6 Настройки параметров коннектора НБКИ-БРС

Для связи с НБКИ необходимо на машине с SSLGate открыть доступ к серверу icrs.nbki.ru по порту 443 напрямую. Если доступ открывается через прокси-сервер, необходимо следовать инструкции «Настройка прокси-соединения для связи сервера Credit Registry с БКИ» в данной документации.

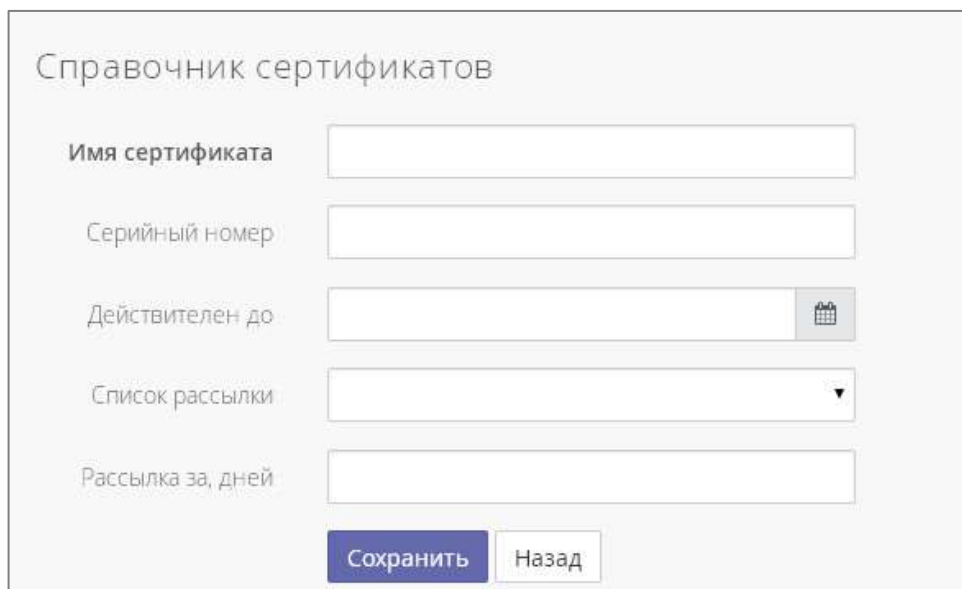
Примечание. Для доступа по http (т.е. для тестового доступа) порт необходимо открывать с сервера с Tomcat.

Прежде чем производить настройку параметров доступа к сервису НБКИ БРС (Бюро Русский Стандарт) рекомендуется ознакомиться с документом «Руководство пользователя Credit Registry».

Примечание: Если у вас уже есть настроенный и работающий коннектор (для одного из сервисов ФМС, ФМС2, ГИБДД, ТСЗ или БРС), и вам нужно настроить другой коннектор из этого списка, то код участника, логин, пароль и сертификат можно скопировать из уже настроенного.

Необходимо выполнить такие действия:


1. На машине с SSLGate установить личный сертификат в сертификаты локального компьютера, следуя инструкции Приложения А. (Личный и корневой сертификаты получают в НБКИ).
2. Войти в систему Credit Registry и добавить серийный номер сертификата в «Справочник сертификатов» (см. «Руководство пользователя Credit Registry»).



Справочник сертификатов

Имя сертификата

Серийный номер

Действителен до 

Список рассылки

Рассылка за, дней

Рис. 15 Добавление сертификата в справочник сертификатов

На закладке «Администрирование» найти раздел «Сертификатов» и воспользоваться кнопкой «добавить» в правом верхнем углу таблицы. Впоследствии введенный номер сертификата необходимо указывать в настройках коннектора.

3. Настроить параметры коннектора.

После добавления нового коннектора для сервиса БРС (Бюро Русский стандарт через НБКИ) устанавливаются следующие параметры:

Добавление профиля коннектора

Коннектор:

Название профиля:

Описание профиля:

Приоритет профиля:

Адрес сервиса:

Код участника:

Имя:

Пароль:

Сертификат:

Максимальное кол-во запросов в ответе по субъекту:

Степень детализации отчета:

Разрешено изменить степень детализации при запросе

Кредитный рейтинг субъекта

Рейтинг вероятности дефолта по юридическому лицу-работодателю

Настройки кэша

Глубина используемого кэша:

Кэшировать несодержательные ответы

Установить запрет на отключение кэша

Настройки соединения с сервисом

Время ожидания ответа сервиса: сек.

Максимальное количество соединений:

Максимальное время ожидания в очереди: сек.

Максимальное время формирования ЭЦП: сек.

Максимальное время установления SSL-соединения: сек.

Расширенные настройки коннектора

Максимальное количество переопытов:

Интервал между переопытами: сек.

Список ошибок, при которых выполнить переопыт:

- ошибка формирования ЭЦП для запросов (SSL Gate)
- таймаут формирования ЭЦП для запросов (SSL Gate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSL Gate
- ошибка/таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 16 Добавление профиля коннектора НБКИ БРС

Параметр	Рекомендации
Коннектор	Содержит название коннектора, автоматически заполняется системой
Название профиля	Содержит название профиля коннектора, заполняется пользователем
Описание профиля	Содержит описание профиля коннектора
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большем числу соответствует больший приоритет.
Адрес БРС сервиса	«Боевой» адрес сервиса: https://icrs.nbki.ru/brs2 Для тестирования и отладки можно использовать адрес: http://brs.demo.nbki.ru:8080/Brs2/brs
Код участника, Имя и Пароль	Информация предоставляется менеджерами НБКИ. Код участника НБКИ имеет последние шесть нулей, имя аналогично коду участника НБКИ, но последние шесть цифр пять нулей и единичка.
Сертификат	Указывается сертификат из выпадающего списка (чтобы сертификат был в списке его необходимо добавить в разделе «Сертификаты» на странице «Администрирование»)
Максимальное количество запросов в ответе по субъекту	Максимальное количество возвращаемых в ответе запросов по указанному субъекту, сделанных ранее
Разрешено изменять степень детализации при запросе (флаг)	Флаг разрешает использование функции изменения степени детализации отчета при запросе
Степень детализации отчета	Выбор степени детализации отчета из выпадающего списка: <ul style="list-style-type: none"> • Максимально детализированный отчет – все данные • Данные о кредитах и своевременности исполнения обязательств за периоды действия договоров • Статистические данные о кредитах • Пустой кредитный отчет. Только рейтинги
Кредитный рейтинг субъекта	При выставленном флаге в ответе возвращается кредитный рейтинг субъекта
Рейтинг вероятности дефолта по юридическому лицу-работодателю	При выставленном флаге в ответе возвращается рейтинг вероятности дефолта по юридическому лицу-работодателю
Настройки кэша	
Глубина используемого кэша	Задается в днях. Перед запросом в бюро Credit Registry просматривает историю запросов. Если такой же запрос повторялся на протяжении последних <глубина кэша> дней, то ответ вернется из кэша.
Кэшировать несодержательные ответы	В истории запросов в любом случае сохраняются все ответы. Но если ответ был несодержательным (бюро ответило ошибкой), то такой запрос вернется из кэша только в случае, когда галочка стоит. Обычно эта опция отключена.

Установить запрет на отключение кэша	Если галочка выставлена, пользователи не смогут делать запросы без использования кэша
Настройки соединения с сервисом	
Время ожидания ответа сервиса	Рекомендуемое значение: 60 с.
Максимальное количество соединений	Рекомендуемое значение: 20.
Максимальное время ожидания в очереди	Рекомендуемое значение: 30 с.
Максимальное время формирования ЭЦП	рекомендуемое значение: 30 с.
Максимальное время установления SSL соединения	Рекомендуемое значение: 30 с.

4. Добавить права на коннектор в ролях тех пользователей, которые будут отправлять запросы, соответствующие сервисы.



Рис. 17 Флаг коннектора НБКИ БРС в списке прав роли

Дополнение:

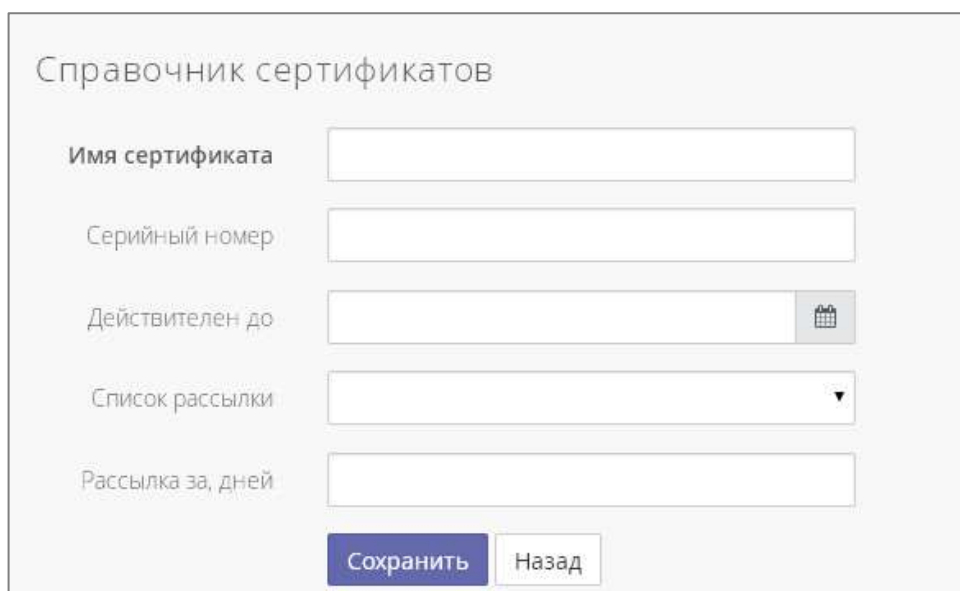
После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение Г. Типичные ошибки настройки коннекторов** (стр. 132).

7.7 Настройка параметров коннектора статистических отчетов НБКИ

Примечание: Если у вас уже есть настроенный и работающий коннектор (для одного из сервисов ФМС, ФМС2, ГИБДД, ТСЗ или БРС, стат. отчеты), и вам нужно настроить другой коннектор из этого списка, то код участника, логин, пароль и сертификат можно скопировать из уже настроенного.

Для настройки запросов статистических отчетов необходимо выполнить следующие действия:


1. На машине с SSLGate установить личный сертификат в хранилище локального компьютера, следуя инструкции «[ПРИЛОЖЕНИЕ А](#)» (личный и корневой сертификаты получают в НБКИ).
2. Войти в систему Credit Registry и добавить серийный номер сертификата в «Справочник сертификатов» (см. «Руководство пользователя Credit Registry»).



Справочник сертификатов

Имя сертификата

Серийный номер

Действителен до 

Список рассылки

Рассылка за, дней

Рис. 18 Добавление сертификата в справочник сертификатов

На закладке «Администрирование» найти раздел «Сертификаты» и воспользоваться кнопкой «добавить» в правом верхнем углу таблицы. Впоследствии введенный номер сертификата необходимо указывать в настройках коннектора.

3. На машине с SSLGate установить в хранилище локального компьютера в папку «Личное» сертификат «СГКО НБКИ – YYYY», где YYYY – год выпуска сертификата (например: «СГКО НБКИ - 2017»). Установка сертификата бюро аналогична установке сертификата удостоверяющего центра, подробнее см. «[ПРИЛОЖЕНИЕ А](#)». Единственное различие - делается импорт в **личные** сертификаты в консоли mmc.
4. Добавить серийный номер сертификата СГКО НБКИ в «справочник сертификатов».
5. Создать на своем почтовом сервере отдельный почтовый ящик для отправки запросов и получения ответов.
6. Добавить и настроить коннектор:

Добавление профиля коннектора

Коннектор: **Статистические отчеты НБКИ**

Название профиля:

Описание профиля:

Приоритет профиля:

Код участника:

Имя пользователя:

Пароль:

Личный сертификат для подписи:

Адрес почты и FTP НБКИ

Адрес e-mail НБКИ для отсылки запросов:

Тема письма с запросом в НБКИ:

Адрес FTP сервера для выкладывания файлов:

Имя пользователя для подключения к FTP:

Пароль для подключения к FTP:

Директория на FTP для файлов:

Адрес e-mail с которого приходит ответы НБКИ:

Сертификат для шифрования:

Настройки почты для получения ответа

Адрес POP3 сервера:

Имя пользователя POP3:

Пароль POP3:

Частота опроса почты: сек

Адрес SMTP сервера:

Имя пользователя SMTP:

Пароль SMTP:

Поле "от" при отправке письма:

Настройки соединения с сервисом

Максимальное время установления SSL соединения: сек

Рис. 19 Добавление профиля коннектора Статистические отчеты НБКИ

Поле	Назначение
Название коннектора	Укажите название профиля коннектора в виде, в котором он будет показан в настройках пользователя.
Описание	Приведите описание данного профиля коннектора в произвольном виде.
Приоритет профиля коннектора	<p>Приоритет используется для того, чтобы определить к какому из профилей коннектора будет обращаться пользователь с несколькими ролями. Из всех назначенных профилей одного пользователя (по каждой из ролей) фактически будет выбираться профиль с наивысшим приоритетом.</p> <p>Опция имеет смысл тогда, когда для одного физического коннектора создаются разные профили настроек, а пользователи системы могут совмещать несколько ролей одновременно.</p>
<p>Аутентификационные данные: (банк получает их у менеджеров НБКИ)</p>	
- Имя пользователя для запросов	Параметр авторизации, передается в НБКИ в xml запросе, как имя автора/пользователя запроса.
- Пароль для запросов	Параметр авторизации, передается в НБКИ в xml запросе, как пароль автора/пользователя запроса.
- Код участника для запросов	Параметр авторизации, передается в НБКИ в xml запросе, как код участника сервиса НБКИ.
- Личный сертификат подписи данных	Личный сертификат пользователя для шифрования ЭЦП запроса.
<p>Адрес почты и FTP НБКИ.</p> <p>Примечание. Загрузка файлов по ftp – устаревший способ загрузки файлов-запросов.</p> <p>На данный момент не используется (на стороне НБКИ).</p> <p>Загрузка файлов больше 7 Мб по https-ссылке на данный момент не реализована.</p>	
Адрес e-mail для отсылки запросов	<p>E-mail НБКИ, на который отсылаются запросы.</p> <p>StatReport@nbki.ru</p>
Тема письма с запросом в НБКИ	<p>Тема письма с запросом.</p> <p>Не проверяется на стороне НБКИ.</p> <p>Можно заполнять произвольно.</p>
Адрес FTP- сервера для выкладывания файлов	<p>Адрес ftp-сервера для загрузки на него больших файлов-запросов (>7 Мб).</p> <p>Адрес вводится без префикса «ftp://»</p> <p>Параметр не используется</p>
Имя пользователя для подключения к FTP	не используются
Пароль для подключения к FTP	

Поле	Назначение
Директория на FTP для файлов	не используется
Адрес e-mail с которого приходят ответы НБКИ	Адрес, с которого приходят ответы от НБКИ. StatReport@nbki.ru Данный адрес служит для фильтрации спама, письма со всех других адресов, кроме указанного, будут игнорироваться.
Сертификат для шифрования данных	Сертификат НБКИ, который используется для отправки запросов в НБКИ. Выбирается из «Справочника сертификатов», куда должен быть загружен ранее. Текущий сертификат СГКО НБКИ
Настройки почты для получения ответов:	
Адрес POP3	Адрес POP3-сервера, на котором находится почтовая запись e-mail-а, для получения ответов на запросы от НБКИ. Примечание: Формат адреса: host:port, где host — сетевой адрес POP3 сервера, port — номер порта POP3 сервера.
Имя пользователя POP3	Авторизация на POP3
Пароль POP3	
Частота опроса почты	Частота опросы почты для выявления ответов от НБКИ, задается в секундах.
Адрес SMTP сервера	Адрес SMTP-сервера, с которого отправляются запросы в НБКИ. Примечание: Формат адреса: host:port, где host — сетевой адрес POP3 сервера, port — номер порта POP3 сервера.
Имя пользователя SMTP	
Имя пользователя SMTP	Авторизация на SMTP
Пароль SMTP	
Поле «от» при отправке письма	Данные, которые будут указываться в поле «От» письма в НБКИ
Прочие настройки:	
Максимальное время установления SSL соединения (сек)	Рекомендуемое значение – 20 сек

Дополнение: После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение G. Типичные ошибки настройки коннекторов** (стр. 132)

7.8 Настройка коннектора НБКИ-AFS

Функции данного коннектора позволяют выявлять в заявлениях на розничные кредиты признаки, указывающие на высокий риск, и таким образом помогает противодействовать недобросовестным заемщикам. Кредитная заявка анализируется и сравнивается со всем массивом заявок, хранящихся в базе данных, ранее переданных и обновляемых участниками проекта.

Настройку коннектора НБКИ-AFS должен проводить пользователь (администратор), у которого установлены права на:

- Редактирование пользователей и прав;
- Редактирование параметров коннектора;
- Редактирование справочник сертификатов.

После добавления нового коннектора устанавливаются следующие параметры:

Добавление профиля коннектора

Коннектор: **НБКИ AFS**

Название профиля:

Описание профиля:

Приоритет профиля:

Адрес сервиса:

Код участника:

Имя:

Пароль:

Название набора правил по умолчанию:

Режим совместимости с Equifax FPS для update

Настройки кэша

Глубина используемого кэша:

Выполнять все запросы без использования кэша

Настройки соединения с сервисом

Время ожидания ответа сервиса: сек

Максимальное количество соединений:

Максимальное время ожидания в очереди: сек

Расширенные настройки коннектора

Максимальное количество переповторов:

Интервал между переповторами: сек

Список ошибок, при которых выполнять переповтор

- ошибка формирования ЭЦП для запросов (SSLGate)
- таймаут формирования ЭЦП для запросов (SSLGate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSLGate
- ошибка/таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 20 Добавление профиля коннектора НБКИ AFS

Параметр	Рекомендации
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большем числу соответствует больший приоритет.
Адрес сервиса	Для боевого доступа: https://icrs.nbki.ru/nbch-afs Тестовый стенд: https://icrs.demo.nbki.ru/nbch-afs
Код участника	Выдают менеджеры НБКИ (последние шесть цифр нули)
Имя	Выдают менеджеры НБКИ (аналогично коду участника НБКИ, но последние шесть цифр пять нулей и единичка)
Пароль	Выдают менеджеры НБКИ
Название набора правил по умолчанию	Наименование набора правил по умолчанию Набор правил необходимо получать в НБКИ
Режим совместимости с Equifax FPS для update	Режим совместимости с Equifax FPS для обновлений
Настройки кэша	
Глубина используемого кэша	Задается в днях. Перед запросом Credit Registry просматривает историю запросов. Если такой же запрос повторялся на протяжении последних <глубина кэша> дней, то ответ вернется из внутренней базы данных, т.е. без запроса бюро.
Выполнять все запросы без использования кэша	При установленной галочке все запросы посредством данного коннектора будут выполняться без использования кэша
Настройки соединения с сервисом	
Время ожидания ответа сервиса	Рекомендуемое значение: 60 сек.
Максимальное количество соединений	Рекомендуемое значение: 20.
Максимальное время ожидания в очереди	Рекомендуемое значение: 30 сек.

Примечания:

- Взаимодействие в рамках данного сервиса происходит в онлайн-режиме.
- Шифрование при обмене данными происходит по протоколу TLS с использованием серверного сертификата («icrs.nbki.ru»).

Обратите внимание, что для обеспечения работы с НБКИ-AFS, пользователям необходимо предоставлять доступ к коннектору через роль. То есть в свойствах роли (закладка «Администрирование» - таблица «Роли» - форма редактирования) в блоке «Доступ к коннекторам» необходимо установить флаг «НБКИ-AFS».

8 Настройка соединения с ОКБ

8.1 Настройка защищенного соединения с ОКБ

1. Проверить, что в закладке «Лицензия» есть строчка «ОКБ», «Экспириан» или «Experian-Interfax». Если этой строчки нет, обратиться к менеджерам для получения лицензии.
2. Проверить, что SSLGate установлен как сервис, то есть в списке служб присутствует служба CreditRegistry SSLGate. Если SSLGate не установлен, то его можно скачать по ссылке: <http://creditregistry.ru/download/SSlgateNet4.17.zip>
3. Установить выданный ОКБ личный сертификат в машинное хранилище в личные сертификаты (см. «[ПРИЛОЖЕНИЕ А](#)»).
4. Установить актуальные корневые сертификаты УЦ КРИПТО-ПРО в хранилище компьютера в «Доверенные корневые центры сертификации».
5. Проверить, установлены ли сертификаты, можно через консоль mmc (см. «[ПРИЛОЖЕНИЕ А](#)», установка сертификатов УЦ, пункты 1-13).

Примечание: Для настройки тестового доступа необходимо установить также сертификат тестового УЦ КРИПТО-ПРО в «доверенные корневые центры сертификации» локального компьютера (импортом через консоль mmc и установку сертификатов УЦ – см. «[ПРИЛОЖЕНИЕ А](#)»). Для тестового доступа также нужны соответствующие корневые сертификаты УЦ КРИПТО-ПРО или тестового УЦ КРИПТО-ПРО.

Примечание: Актуальные сертификаты УЦ КРИПТО-ПРО можно скачать по ссылке: <http://срса20.cryptopro.ru/cacer.p7b>

6. Настроить SSLGate.ini.

Файл C:\Program Files\SSLGate\SSLGate.ini должен иметь вид:

```
[SSLClients]
www.rb-ei.com=серийный_номер_личного_сертификата1
weblink.rb-ei.com=серийный_номер_личного_сертификата2
test.rb-ei.com=серийный_номер_личного_сертификата3
```

Для рабочих запросов должна присутствовать строчка «www.rb-ei.com=...». Для тестовых – «test.rb-ei.com». Строчка «weblink.rb-ei.com» должна быть указана, если настроена автоматическая отправка cds-файлов в ОКБ. Для каждого сайта должен быть вписан серийный номер того личного сертификата, который выдали в ОКБ для соединения с этим сайтом (серийный номер можно посмотреть, открыв сертификат во вкладке «Состав»). Все остальные адреса должны быть закомментированы (знак «;» перед строчкой). Для сертификатов ГОСТ 2012 адрес www.rb-ei.com меняется на ch.bki-okb.com, test.rb-ei.com на ch-test.bki-okb.com, weblink.rb-ei.com на weblink.bki-okb.com.

7. После установки (переустановки) сертификата и изменения SSLGate.ini необходимо перезапустить SSLGate (как сервис).
8. Открыть доступ с машины с SSLGate до www.rb-ei.com по порту 443 напрямую, или через прокси.
9. Если для доступа к серверу БКИ используется прокси-сервер, необходимо следовать инструкции «Настройка прокси-соединения для связи сервера Credit Registry с БКИ» в данной документации.
10. Настроить коннектор ОКБ (EI).

8.2 Настройка коннектора ОКБ в Credit Registry

Настройку системы Credit Registry должен проводить пользователь (администратор), у которого установлены права на:

- редактирование пользователей и прав;
- редактирование параметров коннектора;
- редактирование справочника сертификатов.

После добавления нового коннектора устанавливаются следующие параметры:

Добавление профиля коннектора

Коннектор: ОКБ

Название профиля: Experian

Описание профиля: Experian

Приоритет профиля: 501

Адрес сервиса: https://test.rb-el.com/cpuEnquiry.asp

Подписчик: 803

Группа: MBTC-TEST

запретить использовать одного пользователя для параллельных запросов

Пользователи	Пользователь	Пароль	
	Uzer1	*****	<input type="button" value="добавить"/> <input type="button" value="удалить"/>

Настройки кэша

Глубина используемого кэша: 5

Есть кредитная история	<input type="checkbox"/>
Только запросы	<input type="checkbox"/>
Нет данных	<input type="checkbox"/>
Ошибка	<input type="checkbox"/>

Кэшировать несодержательные ответы

Установить запрет на отключение кэша

Настройки соединения с сервисом

Время ожидания ответа сервиса: 60 сек

Максимальное количество соединений: 5

Максимальное время ожидания в очереди: 10 сек

Максимальное время установления SSL соединения: 10 сек

Расширенные настройки коннектора

Максимальное количество повторов: 0

Интервал между повторами: 30 сек

Список ошибок, при которых выполнять повтор

- ошибка формирования ЭЦП для запросов (SSLGate)
- таймаут формирования ЭЦП для запросов (SSLGate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSLGate
- ошибка/таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 21 Добавление профиля коннектора ОКБ

Параметр	Рекомендации
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большшему числу соответствует больший приоритет.
Адрес сервиса	Для тестового доступа https://test.rb-ei.com/cpuEnquiry.asp Для тестового доступа (ГОСТ 2012) https://ch-test.bki-okb.com/cpuEnquiry.asp Для «боевого» доступа https://www.rb-ei.com/cpuEnquiry.asp Для «боевого» доступа (ГОСТ 2012) https://ch.bki-okb.com/cpuEnquiry.asp
Подписчик Группа Пользователи	Данные, полученные в ОКБ
Запретить использовать одного пользователя для параллельных запросов	В ОКБ не поддерживается выполнение нескольких параллельных запросов от одного пользователя. Данную опцию рекомендуется указывать, если в настройках коннектора используется только один пользователь ОКБ. Если в настройках коннектора указано несколько логинов для подключения к ОКБ, то эта галочка не влияет на схему подключения и в любом случае под каждым логином может быть только одно подключение.
Настройки кэша	
Глубина используемого кэша Есть кредитная история Только запросы Нет данных Ошибка	Задается в днях. Перед запросом в бюро Credit Registry просматривает историю запросов. Если такой же запрос повторялся, то определяется его тип (есть КИ, только запросы, нет данных, ошибка) и выполняется проверка, попадает ли он в заданный интервал кэширования. Если попадает, то ответ возвращается из кэша, иначе выполняется запрос в бюро. Если значение в поле «Есть кредитная история», «Только запросы», «Нет данных» или «Ошибка» не задано, то используется значение из поля «Глубина используемого кэша». Использование кэша позволяет экономить на часто повторяющихся запросах.
Кэшировать несодержательные ответы	В истории запросов в любом случае сохраняются все ответы. Но если ответ был несодержательным (бюро ответило ошибкой), то такой запрос вернется из кэша только в случае, когда галочка стоит. Обычно эта опция отключена.
Установить запрет на отключение кэша	Если галочка выставлена, пользователи не смогут делать запросы без использования кэша
Настройки соединения с сервисом	
Время ожидания ответа сервиса	Рекомендуемое значение: 60 сек.
Максимальное количество соединений	Рекомендуемое значение: должно быть равно количеству максимально разрешенных параллельных подключений под одним логином.

Максимальное время ожидания в очереди	Рекомендуемое значение: 20 сек.
Максимальное время установления SSL-соединения	Рекомендуемое значение: 20 сек.

Для отправки запросов в ОКБ, пользователям необходимо предоставить доступ к коннектору (см. Руководство пользователя Credit Registry, глава 3.3 Роли пользователей):

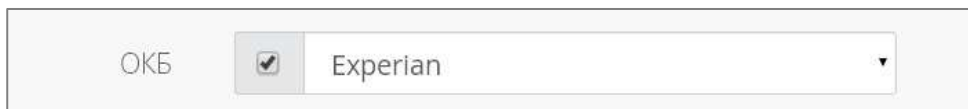


Рис. 22 Флаг коннектора ОКБ в списке прав роли

Рекомендуется в основных параметрах Credit Registry: «Администрирование» -> «Параметры» -> «Основные параметры» -> секция «ОКБ» (см. Руководство пользователя Credit Registry, глава 3.8 Общие настройки системы) установить опцию «Использовать краткую форму отправки запросов»:

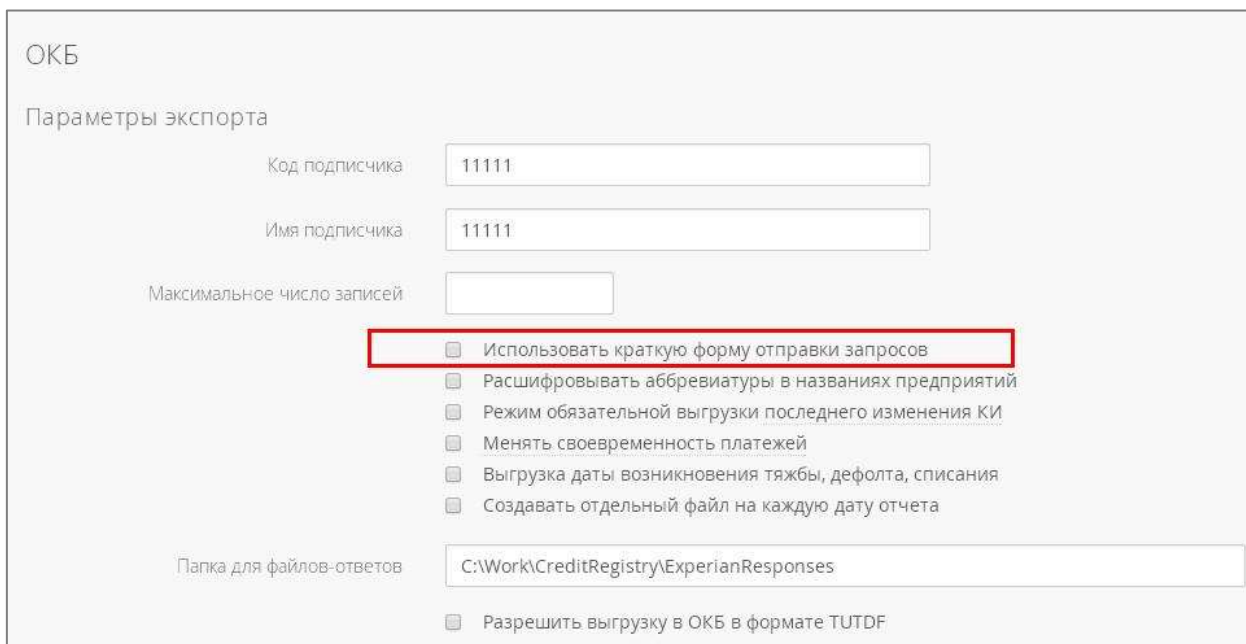


Рис. 23 Параметр «Использовать краткую форму отправки запросов» в параметрах коннектора ОКБ

Замечание: если в «Администрирование» -> «Параметры» -> «Основные параметры» -> блок «Остальные параметры» установить галку «Расширенные настройки коннектора», то у коннектора появятся дополнительные настройки для выполнения повторных запросов в БКИ (при возникновении каких-либо технических ошибок):

Рис. 24 Флаг «Расширенные настройки коннектора» в параметрах системы

Рис. 25 Расширенные настройки коннектора в профиле коннектора

Дополнение: После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение G. Типичные ошибки настройки коннекторов** (стр. 132).

8.3 Настройка сервиса “National Hunter”

Для начала работы с сервисом “National Hunter” необходимо выполнить настройку системы Credit Registry, состоящую из 3 этапов:

8.3.1 Подписание соглашения о вступлении в программу “National Hunter”

После заключения договора с Бюро на предоставление одноименных услуг клиенту предоставляется модуль нормализации, а также ряд параметров для подключения к сервису.

Содержание архива с модулем нормализации выкладывается в произвольную директорию на сервере с Credit Registry.

8.3.2 Создание коннектора National Hunter

Авторизоваться в системе Credit Registry под пользователем, обладающим правами администратора.

Выбрать закладку «Администрирование». В блоке «Профили коннекторов» выбрать значение «National Hunter», после чего нажать кнопку «добавить».



Рис. 26 Кнопка «добавить» в блоке «Профили коннекторов»

Добавление профиля коннектора

Коннектор: **National Hunter**

Название профиля:

Описание профиля:

Приоритет профиля:

Идентификатор клиента:

Название клиента:

Схемы сравнения: (через ,)

Использовать все схемы, если ни одной не указано

Адрес online matching сервиса National Hunter:

Адрес сервиса смены пароля National Hunter:

Имя пользователя:

Пароль:

Смена пароля каждые 80 дней

Следующая смена пароля:

Настройки кэша

Глубина используемого кэша:

Кэшировать несодержательные ответы

Выполнить все запросы без использования кэша

Настройки соединения с сервисом

Время ожидания ответа сервиса: сек

Максимальное время установления SSL соединения: сек

Расширенные настройки коннектора

Максимальное количество переповторов:

Интервал между переповторами: сек

Список ошибок, при которых выполнять переповтор

- ошибка формирования ЭЦП для запросов (SSLGate)
- таймаут формирования ЭЦП для запросов (SSLGate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSLGate
- ошибка/таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 27 Добавление профиля коннектора National Hunter

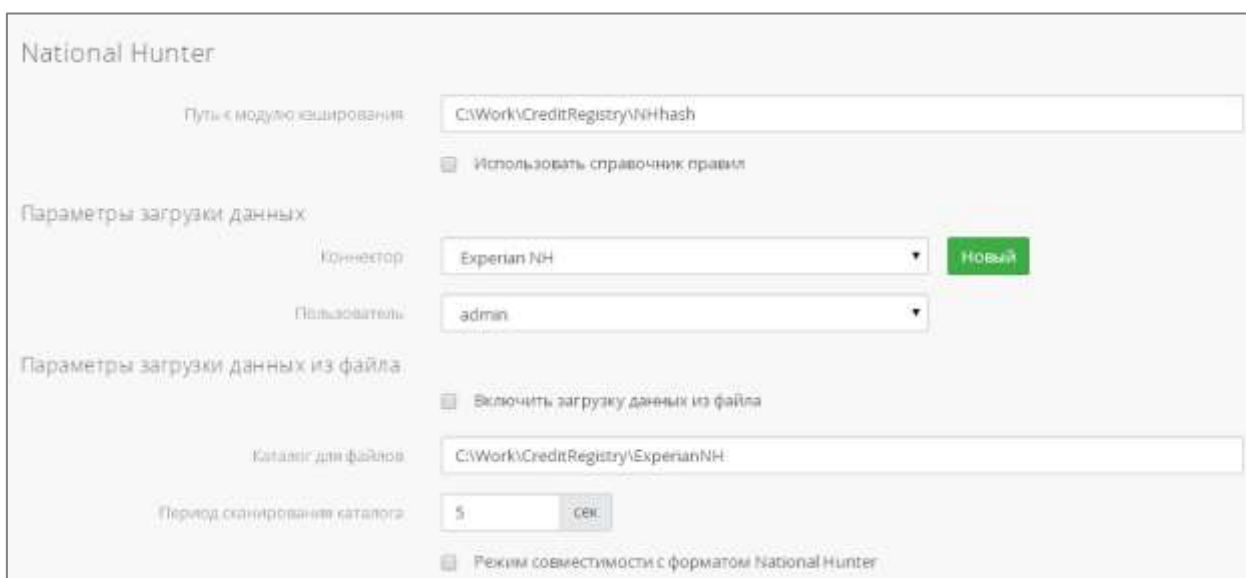
Параметр	Рекомендации
Название коннектора	Произвольное название
Описание	Произвольное описание
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большем числу соответствует больший приоритет.
Идентификатор клиента сервиса NH	Данную информацию предоставляет бюро.
Название клиента сервиса NH	Данную информацию предоставляет бюро.
Схемы сравнения (через запятую)	Данную информацию предоставляет бюро.
Использовать все схемы, если ни одной не указано	Флаг учитывает использование все схемы, если ни одной не указано
Адрес online matching сервиса National Hunter	Тестовый: https://nh-test.rb-ei.com/OnlineMatchingService/OnlineMatching.asmx Боевой: https://nh.rb-ei.com/OnlineMatchingService/OnlineMatching.asmx
Адрес сервиса смены пароля National Hunter	Тестовый: https://nh-test.rb-ei.com/EIHunterManager/passwords.asmx Боевой: https://nh.rb-ei.com/EIHunterManager/passwords.asmx
Имя пользователя	Данную информацию предоставляет бюро
Пароль	Данную информацию предоставляет бюро
Смена пароля каждые 25 дней	Рекомендовано выставить данный флаг
Следующая смена пароля	Указывается дата в формате ДД.ММ.ГГГГ следующей смены пароля
Настройки кэша	
Глубина используемого кэша	Задается в днях. Перед запросом Credit Registry просматривает историю запросов. Если такой же запрос повторялся на протяжении последних <глубина кэша> дней, то ответ вернется из внутренней базы данных, т.е. без запроса бюро.
Кэшировать несодержательные ответы	Установленный флаг активирует кэширование несодержательных ответов
Выполнять все запросы без использования кэша	При установленном флаге запросы выполняются без использования кэша
Настройки соединения с сервисом	
Время ожидания ответа сервиса (сек)	Рекомендуемое значение: 30
Максимальное время установления SSL соединения (сек)	Рекомендуемое значение: 20

Дополнение: После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение G. Типичные ошибки настройки коннекторов** (стр. 132).

8.3.3 Настройка параметров сервиса

Авторизоваться в системе Credit Registry под пользователем, обладающим правами администратора.

Выбрать закладку «Администрирование». В блоке «Параметры» выбрать «Основные параметры», найти секцию «National Hunter»:



National Hunter

Путь к модулю хеширования: C:\Work\CreditRegistry\NH\hash

Использовать справочник правил

Параметры загрузки данных

Коннектор: Experian NH

Пользователь: admin

Параметры загрузки данных из файла

Включить загрузку данных из файла

Каталог для файлов: C:\Work\CreditRegistry\ExperianNH

Период сканирования каталога: 5 сек.

Режим совместимости с форматом National Hunter

Рис. 28 Настройки NH в основных параметрах системы

Параметр	Описание
Путь к модулю хэширования	Путь к модулю нормализации – указывается корневой каталог в котором располагается RFPS.jar. Архив с модулем нормализации предоставляет бюро.
Параметры загрузки данных	
Коннектор	Название коннектора для обмена данными с сервисом “Национальный хантер”
Пользователь	Имя пользователя, от имени которого будет выполняться первоначальная загрузка, а также дальнейшие запросы через CSV файлы. Описание формата файлов высылается при необходимости.
Параметры загрузки данных из файла	
Включить загрузку данных из файла	Флаг, активирующий загрузку данных из CSV файла
Каталог для файлов	Директория для размещения CSV файлов
Период сканирования каталога, сек	Период сканирования директории на предмет появления новых файлов
Режим совместимости с форматом National Hunter	Поддержка формата CSV файла с кодировкой UTF-8 и разделителем запятой

В SSLGate.ini необходимо добавить строчку вида:

"nh-test.rb-ei.com = номер сертификата"

(где имя хоста должно быть такое же, как и в адресе в настройках коннектора, номер сертификата такой же, как и для основных запросов)

После изменения SSLGate.ini необходимо перезапустить сервис SSLGate.

Перед запросами через Credit Registry необходимо убедиться, что на стороне ОКБ внешний IP-адрес, с которого осуществляются запросы, внесен в список разрешенных. В противном случае при попытке зайти на сайт <https://nh-test.rb-ei.com/OnlineMatchingService/OnlineMatching.aspx> через Internet Explorer будет выдаваться ошибка:

HTTP Error 403.6 - Forbidden: IP address of the client has been rejected. Internet Information Services (IIS)

Для начала работы пользователей, им необходимо предоставить доступ к коннектору (см. Руководство пользователя Credit Registry, глава 3.3 Роли пользователей):

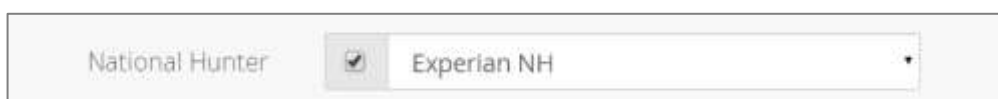


Рис. 29 Флаг NH в списке прав роли

Перед первым запросом необходимо сменить пароль в настройках коннектора:

Redaction of connector profile

Коннектор	National Hunter
Название профиля	Experian NH
Описание профиля	Experian NH Production
Приоритет профиля	1
Идентификатор клиента	10
Название клиента	client
Схемы сравнения	7,8 <small>(через ,)</small>
	<input type="checkbox"/> Использовать все схемы, если ни одной не указано
Адрес online matching сервиса National Hunter	http://INFO010-8089/mockMatchingSoap
Адрес сервиса смены пароля National Hunter	http://INFO010-8090/mockChangePasswordSoap
Имя пользователя	client
Пароль	***** Сменить пароль
	<input type="checkbox"/> Смена пароля каждые 80 дней
Следующая смена пароля	<input type="text"/>

Рис. 30 Смена пароля в настройках коннектора NH

Дополнение: После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение G. Типичные ошибки настройки коннекторов** (стр. 132).

9 Настройка соединения с Эквифакс Кредит Сервисиз

9.1 Настройка защищенного соединения с Эквифакс

Внимание: Для запросов в БКИ «Эквифакс Кредит Сервисиз» (бывшее ГПКС) с использованием Credit Registry настоятельно рекомендуется использовать ключ и сертификат CryptoPro (а не FilePro). О создании ключей и сертификатов необходимо заранее уведомить технических сотрудников БКИ «Эквифакс».

Для запросов в Equifax необходимо:

1. Реализовать доступ с машины, на которой установлена Credit Registry, на сайт Equifax.

При стандартных настройках используются следующие внутренние IP-адреса в сети Equifax:
http://10.130.1.2 – тестовый доступ; http://10.130.10.130 – «боевой» доступ.

Для доступа на этот сайт необходимо **совместно с техподдержкой Equifax** настроить vpn-канал (vpn может быть настроен либо программно, либо аппаратно с помощью дополнительного оборудования VPN-Gate; для Credit Registry не имеет значения, каким из этих способов будет настроен vpn).

Проверить корректность настройки vpn-канала, можно открыв сайт Equifax в Internet Explorer (не ниже 8й версии).

Пока зайти на сайт Equifax с машины с Credit Registry через браузер нельзя, vpn настроен не полностью.

2. Получить личный сертификат CryptoPro для подписи.

Примечание: необходимо использовать именно сертификат CryptoPro(*а не FilePro*). Во время генерации запроса на сертификат не следует выбирать опцию «усиленная защита ключа», также предпочтительно пометить ключ как экспортируемый.

3. Настроить SSLGate. Дистрибутив доступен для скачивания по ссылке:
<http://creditregistry.ru/download/SSlgateNet4.17.zip>
4. Установить личный сертификат в машинное хранилище сертификатов в личные сертификаты, как описано в Приложении А.
5. Настроить коннектор к Equifax в программе Credit Registry.

(Администрирование -> Профили коннекторов -> Добавить)

9.2 Настройка коннектора Эквифакс в Credit Registry

Рекомендации по настройке параметров приведены ниже в таблице.

Добавление профиля коннектора

Коннектор: **ЭквиФакс**

Название профиля:

Описание профиля:

Приоритет профиля:

Код партнера:

Адрес сервиса для запросов по физ. лицам:

Тип счета для запросов по физ. лицам:

Платеж дополнительных εργαбутов:

Адрес сервиса для запросов по юр. лицам:

Тип счета для запросов по юр. лицам:

Личный сертификат (для подписи запросов):

Версия формата запроса:

Настройки кэша

Глубина используемого кэша:

Есть кредитная история	<input type="text"/>
Только запросы	<input type="text"/>
Нет данных	<input type="text"/>
Ошибка	<input type="text"/>

Кэшировать несодержательные ответы

Установить запрет на отключение кэша

Настройки соединения с сервисом

Время ожидания ответа сервиса: сек

Максимальное количество соединений:

Максимальное время ожидания в очереди: сек

Максимальное время формирования ЭЦП: сек

Расширенные настройки коннектора

Максимальное количество переполюторов:

Интервал между переполюторами: сек

Список ошибок, при которых выполнить переполютор

- ошибка формирования ЭЦП для запросов (SSLGate)
- таймаут формирования ЭЦП для запросов (SSLGate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSLGate
- ошибка таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 31 Добавление профиля коннектора ЭквиФакс

Параметр	Рекомендации
Тип коннектора	Содержит тип коннектора, автоматически заполняется системой
Название коннектора	Содержит название коннектора, заполняется администратором
Описание	Содержит описание коннектора, заполняется администратором
Приоритет профиля коннектора	Содержит число: чем больше число, тем больше приоритет
Код партнера, используется для взаимодействия с Эквифакс	Данные, полученные в Equifax
Адрес Эквифакс сервиса для запросов по физ. лицам	Адрес согласовывается с техподдержкой Equifax. Если доступ настроен стандартно, то http://10.130.1.2/xml.php - тестовый доступ; http://10.130.10.130/xml.php - «боевой» доступ.
Тип отчета, используемый по умолчанию для запросов по физ. лицам	Указывается тип отчета Эквифакс для версий 2.0 и 3.0 для запросов по физ. лицам (данные, полученные в Equifax)
Пакеты доп. атрибутов	Параметр задает пакеты дополнительных атрибутов. Символ «;» - разделитель между пакетами, символ «-» - разделитель между значением и названием, например: «123-пакет доп. атрибутов 123; 1234-пакет доп. атрибутов 1234»
Адрес Эквифакс сервиса для запросов по юр. лицам	Содержит адрес сервиса для запросов по юр. лицам
Тип отчета, используемый по умолчанию для запросов по юр. лицам	Указывается тип отчета Эквифакс для версий 2.0 и 3.0 для запросов по юр. лицам (данные, полученные в Equifax)
Серийный номер личного сертификата (для подписи запросов)	Личный сертификат, полученный в Equifax. Сертификат должен быть прописан в справочнике сертификатов в Credit Registry (администрирование, справочник сертификатов), а также установлен на сервере с SSLGate. См. « ПРИЛОЖЕНИЕ А ».
Версия формата запроса	Формат запросов нужно определить с техподдержкой Equifax (2.0 или 3.0).
Настройки кэша	
Глубина используемого кэша Есть кредитная история Только запросы Нет данных Ошибка	Задается в днях. Перед запросом в бюро Credit Registry просматривает историю запросов. Если такой же запрос повторялся, то определяется его тип (есть КИ, только запросы, нет данных, ошибка) и выполняется проверка, попадает ли он в заданный интервал кэширования. Если попадает, то ответ возвращается из кэша, иначе выполняется запрос в бюро.

Параметр	Рекомендации
	Если значение в поле «Есть кредитная история», «Только запросы», «Нет данных» или «Ошибка» не задано, то используется значение из поля «Глубина используемого кэша». Использование кэша позволяет экономить на часто повторяющихся запросах.
Кэшировать несодержательные ответы	В истории запросов в любом случае сохраняются все ответы. Но если ответ был несодержательным (бюро ответило ошибкой), то такой запрос вернется из кэша только в случае, когда галочка стоит. Обычно эта опция отключена
Установить запрет на отключение кэша	Если галочка выставлена, пользователи не смогут делать запросы без использования кэша
Настройки соединения с сервисом	
Время ожидание ответа БКИ (сек)	Рекомендуемое значение: 60 сек.
Максимальное количество подключений к БКИ	Рекомендуемое значение: 30.
Максимальное время ожидания в очереди (сек)	Рекомендуемое значение: 15 сек.
Максимальное время формирования ЭЦП (сек)	Рекомендуемое значение: 60 сек.
Расширенные настройки коннектора	
Расширенные настройки коннектора Максимальное количество переповторов Интервал между переповторами (сек) Список ошибок, при которых выполнять переповтор	Данный блок настроек отображается, если в «Администрирование» -> «Параметры» -> «Основные параметры» -> секция «Остальные настройки» стоит галочка у параметра «Расширенные настройки коннектора»

Рекомендуем также настроить обновление схем Equifax. Схемы Equifax - это схемы отображения отчета в html и в pdf. Их можно скачивать с сервера Equifax вручную, либо автоматически.

Для настройки обновления схем Equifax:

- У администратора системы установить право «Право на запуск (и редактирование расписания) обновления схем Equifax»:

<input type="checkbox"/>	Запретить делать запросы (только просмотр истории)
<input type="checkbox"/>	Запретить запрашивать физические лица
<input type="checkbox"/>	Запретить запрашивать юридические лица
<input checked="" type="checkbox"/>	Редактирование профиля коннектора
<input checked="" type="checkbox"/>	Право на запуск (и редактирование расписания) обновления схем Equifax

Рис. 32 Право «Право на запуск (и редактирования расписания) обновления схем Equifax»

Примечание: прежде чем выполнить следующий пункт, убедитесь, что у вас установлено право «[Редактирование дополнительных атрибутов](#)»:

Основные параметры

Название роли	<input type="text" value="admin"/>
Описание роли	<input type="text" value="Роль для пользователя [admin]"/>
Приоритет роли	<input type="text" value="0"/> (0-1000)

- Редактирование пользователей и прав
- Редактирование дополнительных параметров
- Редактирование группы
- Редактирование справочника кредитных программ
- Редактирование кода участника НБКИ
- Редактирование РНКО (ЦБ ЦККИ)
- Редактирование справочника ТУ и филиалов
- Редактирование справочника сертификатов
- Редактирование списков рассылок
- Редактирование стратегий триггеров
- Групповые запросы
- Пакетные запросы

Рис. 33 Право «Редактирование дополнительных параметров»

- Заполните раздел «Обновление схем Equifax» в блоке параметров «Эквифакс» в «Основных настройках»:

Эквифакс

Отключить кэширование по типу запрашиваемого отчета

Обновление схем Эквифакс

Директория для хранения

Время обновления схем

URL файла FOP	v2.0	<input type="text" value="http://10.130.10.130/fop.xsl"/>
	v3.0	<input type="text" value="http://10.130.10.130/schema_3.0.fop"/>
URL файла XSLT	v2.0	<input type="text" value="http://10.130.10.130/schema.xsl"/>
	v3.0	<input type="text" value="http://10.130.10.130/schema_3.0.xsl"/>

Рис. 34 Блок параметров для обновления схем Эквифакс

«Директория для хранения» – обязательный параметр, произвольная директория, в которую будут сохраняться схемы.

Адреса для скачивания схем уточняются у сотрудников Equifax. В случае стандартных настроек доступа к сайту Equifax:

FOP URL для Эквифакс 2.0 (для генерации pdf)	http://10.130.10.130/fop.xsl
FOP URL для Эквифакс 3.0 (для генерации pdf)	http://10.130.10.130/schema_3.0.fop
XSLT URL для Эквифакс 2.0 (для генерации html)	http://10.130.10.130/schema.xsl
XSLT URL для Эквифакс 3.0 (для генерации html)	http://10.130.10.130/schema_3.0.xsl

Примечание: IP-адрес указан для стандартных настроек. Если в коннекторе Equifax указывается адрес, отличный от 10.130.10.130, то нужно указывать его в адресах для скачивания схем.

«Время обновления схем» – если указано, то схемы будут обновляться ежедневно автоматически. Если поле не заполнено, обновлять схемы следует вручную – с помощью кнопки **«Обновление схем Equifax»** в блоке **«Параметры»** на странице **«Администрирование»**.

1. В ролях пользователей дать права на коннектор Equifax.
2. Зайти на закладку Equifax, сделать запрос.

Замечание: если в **«Администрирование»** → **«Параметры»** → **«Основные параметры»** → секция **«Остальные настройки»** установить галку **«Расширенные настройки коннектора»**, то у коннектора появятся дополнительные настройки для выполнения повторных запросов в БКИ (при возникновении каких-либо технических ошибок):

Расширенные настройки коннектора

Максимальное количество переповторов

Интервал между переповторами сек

Список ошибок, при которых выполнять переповтор

- ошибка формирования ЭЦП для запросов (SSLGate)
- таймаут формирования ЭЦП для запросов (SSLGate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSLGate
- ошибка/таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 35 Расширенные настройки коннектора

Дополнение: После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение G. Типичные ошибки настройки коннекторов** (стр. 132).

9.3 Настройка Equifax FPS

Для того чтобы начать работу с коннектором Equifax FPS, необходимо выполнить действия, описанные ниже.

- 1) Авторизоваться в системе Credit Registry под пользователем, обладающим правами администратора.
- 2) Перейти в раздел «Администрирование» -> «Профили коннекторов», нажать кнопку «Добавить»:

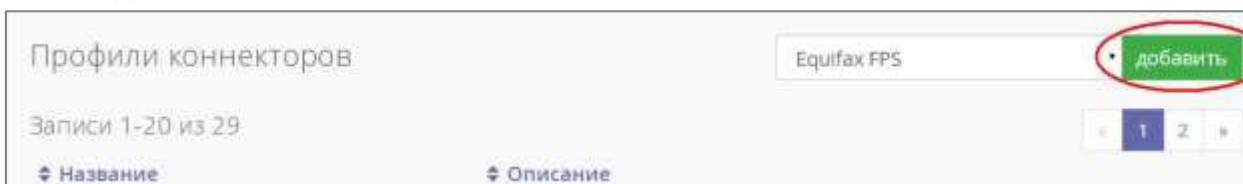


Рис. 36 Кнопка «Добавить» в разделе «Профили коннекторов»

- 3) Заполнить форму «Добавление профиля коннектора»:

Добавление профиля коннектора

Коннектор:

Название профиля:

Описание профиля:

Приоритет профиля:

Адрес сервиса:

Включить поддержку версии FPS 2.0.

Точка входа веб-сервиса FPS для передачи фотографии:

Идентификатор партнера Equifax:

Имя пользователя ЛБД:

Пароль пользователя ЛБД:

Настройки соединения с сервисом

Время ожидания ответа от сервиса: сек

Максимальное количество подключений к сервису:

Количество попыток запроса выходного вектора:

Время до первой попытки запроса выходного вектора: сек (По умолчанию 0)

Настройки кэша

Глубина используемого кэша:

Кэшировать несодержательные ответы

Установить запрет на оплоучение кэша

Выполнять все запросы без использования кэша

Расширенные настройки коннектора

Максимальное количество переповторов:

Интервал между переповторами: сек

Список ошибок, при которых выполнять переповтор

- ошибка формирования ЭЦП для запросов (SSLGate)
- таймаут формирования ЭЦП для запросов (SSLGate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSLGate
- ошибка/таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 37 Добавление профиля коннектора Equifax FPS

Форма состоит из следующих полей:

Имя	Комментарий
Тип коннектора	Equifax FPS
Название профиля	Equifax FPS
Описание профиля	Заполняется произвольным образом для удобства пользования коннектором
Приоритет профиля	Число. Чем больше число, тем выше приоритет коннектора
Адрес сервиса	Данные, полученные из Equifax. Ссылка должна быть следующего вида: http://адрес.полученный.в.эквифакс/soap/bank
Включить поддержку версии FPS 2.0	Активирует поддержку Equifax FPS версии 2.0
Точка входа веб-сервиса FPS для передачи фотографии	Адрес сервиса для передачи биометрических данных
Идентификатор партнера Equifax	Данные, полученные Equifax
Имя пользователя ЛБД	Задается исходя из настроек в разделе «Основные параметры»
Пароль пользователя ЛБД	Задается исходя из настроек в разделе «Основные параметры»
Настройка соединения с сервисом	
Время ожидания ответа от сервиса	Время ожидания ответа от сервиса в секундах
Максимальное количество подключений к сервису	Содержит число – максимальное количество подключений
Кол-во попыток запроса выходного вектора	Рекомендуемое значение - 10
Время до первой попытки запроса выходного вектора	Время в секундах до первой попытки запроса выходного вектора (по умолчанию 8). Дальнейшие попытки будут выполняться каждую секунда
Настройки кэша	
Глубина используемого кэша	Ответы из кэша будут возвращаться за последние n дней
Кэшировать несодержательные ответы	Несодержательные ответы отправлять в кэш

Установить запрет на отключение кэша	Если галочка выставлена, пользователи не смогут делать запросы без использования кэша
Выполнять все запросы без использования кэша	Ответы из кэша возвращаться не будут

После заполнения формы необходимо нажать **«Сохранить»**.

- 4) Настроить подключение к БД для сохранения отчетов.
 Для этого перейти на страницу **«Администрирование»** -> **«Параметры»** -> **«Основные параметры»** секция **«Настройки подключения к Базам Данных для сохранения отчетов»** (Сохранение отчетов) -> в списке **«Выгрузка унифицированных отчетов»** поставить флаг напротив поля **«Equifax FPS»**

Настройки подключения к Базам Данных для сохранения отчетов

Интервал опроса очереди отчетов: сек. (от 3 до 120)

- Выгрузка по таблице **REPORTS_TO_SAVE**
- После выгрузки в бд устанавливать для потоковых запросов статус 3
- Выгрузка запросов из кэша
- Выгрузка запросов с ошибками

Выгрузка унифицированных отчетов

- НБКИ
- Эквифакс
- ОКБ
- ФМС
- НБКИ-БРС
- БРС
- Equifax FPS**
- National Hunter
- Кронос
- СМЭВ ФМС
- Мегафон
- Спарк
- ПФР

Рис. 38 Настройки подключения к БД для сохранения отчетов

- 5) В секции для отчетов **«Equifax FPS»** указать значения полей **«URL»** и **«Имя пользователя»**

Equifax FPS

Выгрузка в онлайн

URL

Имя Пароль

Рис. 39 Секция для отчетов Equifax

При необходимости проставить флаг **«Выгрузка в онлайн»** и заполнить поле **«Пароль»**

6) Указать параметры загрузки данных в секции «Параметры загрузки данных».

The screenshot shows the configuration interface for Equifax FPS. It is divided into several sections:

- Equifax FPS**:
 - Путь к файлу хэширования: [Empty text box]
 - Использовать справочник правил
 - Альтернативный режим работы с датой заявки
- Параметры загрузки данных**:
 - Коннектор: [Equifax FPS] [Новый]
 - Пользователь: [admin]
- Параметры загрузки данных из файла**:
 - Включить загрузку данных из файла
 - Каталог для файлов: [C:\Work\CreditRegistry\EquifaxFPS]
 - Период сканирования каталога: [5] сек
- Параметры загрузки данных из СУБД**:
 - Включить загрузку данных из БД
 - URL: [Empty text box]
 - Имя: [Empty text box] | Пароль: [Empty text box]
 - Период сканирования БД: [5] сек

Рис. 40 Параметры загрузки данных Equifax FPS

10 Настройка соединения с БРС

10.1 Настройка защищенного соединения с БРС

1. Проверить, что в закладке «лицензия» есть строчка «БРС». Если этой строчки нет, обратиться к менеджерам для получения лицензии.
2. Проверить, что SSLGate установлен как сервис, то есть в списке служб присутствует служба CreditRegistry SSLGate. Если SSLGate не установлен, то его можно скачать по ссылке: <http://creditregistry.ru/download/SSlgateNet4.17.zip>
3. Установить выданный БРС личный сертификат в хранилище компьютера в личные сертификаты (см. «[ПРИЛОЖЕНИЕ А](#)»).
4. Актуальные корневые сертификаты УЦ КРИПТО-ПРО в хранилище компьютера в «Доверенные корневые центры сертификации».
5. Проверить, установлены ли сертификаты, можно через консоль mmc (см. «[ПРИЛОЖЕНИЕ А](#)», установка сертификатов УЦ, пункты 1-13).

Примечание: Для настройки тестового доступа необходимо установить также сертификат тестового УЦ КРИПТО-ПРО в хранилище компьютера в «Доверенные корневые центры

сертификации» (импортом через консоль mmc и установку сертификатов УЦ, см. «[ПРИЛОЖЕНИЕ А](#)»). Для тестового доступа также нужны корневые сертификаты УЦ КРИПТО-ПРО, и сертификат тестового центра КРИПТО-ПРО.

Примечание: Актуальные сертификаты УЦ КРИПТО-ПРО можно скачать по ссылке: <http://cpsa20.cryptopro.ru/cacer.p7b>.

6. Настроить SSLGate.ini.

Файл C:\Program Files\SSLGate\SSLGate.ini должен содержать строки:

```
[SSLClients]
crs.rs-cb.ru= серийный номер личного сертификата
```

Для рабочих запросов должна присутствовать строка «crs.rs-cb.ru=... ». Для тестовых – «test-crs.rs-cb.ru». Для сертификатов ГОСТ 2012 адрес crs.rs-cb.ru меняется на crs12.rs-cb.ru, test-crs.rs-cb.ru на crs12-test.rs-cb.ru. Для каждого сайта должен быть вписан серийный номер того личного сертификата, который выдали в БРС для соединения с этим сайтом (серийный номер можно посмотреть, открыв сертификат во вкладке «Состав»). Все остальные адреса должны быть закоментированы (знак «;» перед строкой).

- После установки (переустановки) сертификата и изменения SSLGate.ini необходимо перезапустить SSLGate (как сервис).
- Открыть доступ с машины с SSLGate до crs.rs-cb.ru по порту 443 напрямую или через прокси.

Если для доступа к серверу БКИ используется прокси-сервер, необходимо следовать инструкции «Настройка прокси-соединения для связи сервера Credit Registry с БКИ» в данной документации.

7. Настроить коннектор БРС.

10.2 Настройка коннектора БРС в Credit Registry

Настройку системы Credit Registry должен проводить пользователь (администратор), у которого установлены права на:

- редактирование пользователей и прав;
- редактирование параметров коннектора;

После добавления нового коннектора устанавливаются следующие параметры:

Добавление профиля коннектора

Коннектор: БРС

Название профиля: БРС

Описание профиля: Русский стандарт

Приоритет профиля: 1

Адрес сервиса: https://test-crs.rs-cb.ru/A2A/request.asfx

Адрес сервиса верификации: https://test-crs.rs-cb.ru/A2A/request.asfx

Имя пользователя: ЭО

Название организации: Закрытое акционерное общество «МТЦ»

Максимальное кол-во запросов в ответе по субъекту: 100

Степень детализации отчета:

- Разрешено изменить степень детализации при запросе
- Кредитный рейтинг субъекта
- Рейтинг вероятности дефолта по юридическому лицу-работодателю
- Не передавать данные о работодателе для всех запросов кроме Рейтинг 2
- Сервис верификации

Настройки кэша

Глубина используемого кэша:

Есть кредитная история	
Только запросы	
Нет данных	
Ошибка	

Кэшировать несоответствующие ответы

Установить запрет на отключение кэша

Настройки соединения с сервисом

Время ожидания ответа сервиса: сек

Максимальное количество соединений:

Максимальное время ожидания в очереди: сек

Максимальное время установления SSL соединения: сек

Расширенные настройки коннектора

Максимальное количество переопределений: 0

Интервал между переопределениями: 30 сек

Список ошибок, при которых выполнять переопределение:

- ошибка формирования ЭЦП для запросов (SSLGate)
- таймаут формирования ЭЦП для запросов (SSLGate)
- таймаут ожидания в очереди коннектора
- ошибки соединений с SSLGate
- ошибки/таймаут соединений с БКИ
- таймаут ответа БКИ или внешнего источника
- прочие сетевые ошибки
- ошибка БКИ или внешнего источника в прикладном протоколе

Рис. 41 Добавление профиля коннектора БРС

Параметр	Рекомендации
Название профиля	Название профиля коннектора
Описание профиля	Описание профиля коннектора
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большшему числу соответствует больший приоритет.
Адрес сервиса	Для тестового доступа https://crs-test.rs-cb.ru/A2A/request.ashx Для тестового доступа (ГОСТ 2012) https://crs12-test.rs-cb.ru/A2A/request.ashx Для «боевого» доступа https://crs.rs-cb.ru/A2A/request.ashx Для «боевого» доступа (ГОСТ 2012) https://crs12.rs-cb.ru/A2A/request.ashx
Адрес сервиса верификации	Содержит тот же адрес что и поле «Адрес БРС-сервиса»
Имя пользователя Название организации	Данные, полученные в БРС
Максимальное кол-во запросов в ответе по субъекту	Максимальное количество возвращаемых в ответе запросов по указанному субъекту, сделанных ранее
Разрешено изменять степень детализации при запросе	Если данная опция включена, пользователь при запросе сможет менять детализацию отчета
Степень детализации отчета (если не разрешено изменять)	Доступные значения: - Максимально детализированный отчет - все данные - Статистические данные о кредитах и своевременность исполнения обязательств за периоды действия договоров - Статистические данные о кредитах - Пустой кредитный отчет - значение может быть использовано, например, для получения только рейтингов
Настройки кэша	
Глубина используемого кэша	Задается в днях. Перед запросом в бюро Credit Registry просматривает историю запросов. Если такой же запрос повторялся на протяжении последних <глубина кэша> дней, то ответ вернется из кэша. Использование кэша позволяет экономить на часто повторяющихся запросах.
Кэшировать несодержательные ответы	При установленном флаге кэшируются несодержательные ответы
Установить запрет на отключение кэша	Если галочка выставлена, пользователи не смогут делать запросы без использования кэша
Настройки соединения с сервисом	
Время ожидания ответа сервиса	Рекомендуемое значение: 60 сек.
Максимальное количество соединений	Рекомендуемое значение: 30.
Максимальное время ожидания в очереди	Рекомендуемое значение: 15 сек.
Максимальное время установления SSL соединения	Рекомендуемое значение: 20 сек.

Для отправки запросов в БРС, пользователям необходимо предоставить доступ к коннектору (см. Руководство пользователя Credit Registry, глава 3.3 Роли пользователей):

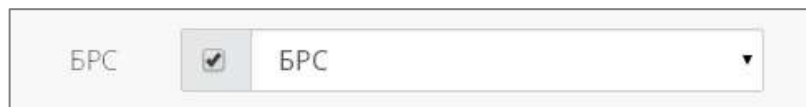


Рис. 42 Флаг коннектора БРС в списке прав роли

Дополнение: После настройки коннектора выполните запрос. Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение Г. Типичные ошибки настройки коннекторов** (стр. 132).

11 Настройка соединения с ЦККИ

Запросы в ЦККИ могут осуществляться несколькими способами:

- Почта X.400 (необходим почтовый ящик на сервере REX400 и "Вербовские" ключи; платная часть - шлюз через REX400)
- система СВК (необходимы "вербовские" ключи и доступ в сеть СВК)
- директории отправки банковской отчетности (Credit Registry выкладывает запрос в директорию запросов, забирает ответ из директории ответов. Подписание, шифрование и отправка запросов осуществляются не с помощью Credit Registry, а внешним ПО. Запросы могут отправляться точно так же, как и банковская отчетность, подготавливаемая для ЦБ)
- сервис АСЭП (устаревающий, не рекомендуемый вариант)
- сервис АСТРА (устаревающий, не рекомендуемый вариант)
- запросы через НБКИ ("Вербовские" ключи не требуются, необходим личный сертификат для запросов в НБКИ, запросы платные)

Примечание: здесь указаны только основные способы подключения и основные различия. Полное описание - ниже.

Если вместо Tomcat используется WebSphere AS, необходимо проверить, что в папку с WebSphere был добавлен mail-1.4.jar, а также был создан объект java mail library и приложение Credit Registry было настроено на использование этой библиотеки. Подробнее эти действия описаны в руководстве по установке Credit Registry на WebSphere.

11.1 Настройка запросов ЦККИ через почту X400

Credit Registry не поддерживает отправку почты в формате X.400. Тем не менее, данный вариант отправки запросов возможен (и реализован в нескольких банках): Credit Registry осуществляет отправку и получение данных по обычной internet-почте (по протоколам SMTP и POP3), шлюз из обычной internet-почты в почту X.400 обеспечивает сам банк. В данной документации описан вариант, когда в качестве шлюза из SMTP/POP3 в почту в формате X.400 выступает «Клуб-400» (<http://rex400.ru>).

На сервере REX400 необходимо создать почтовый ящик. Credit Registry будет подключаться к серверу «Клуб-400» по стандартным протоколам SMTP и POP3, а почтовый сервер будет отправлять письма-запросы в ЦККИ в формате X.400.

Необходимая информация и компоненты:

- 1) информационное письмо ЦБ, содержащее регистрационный номер кредитной организации, присвоенный банку.
- 2) Учетная запись на почтовом сервере REX400 для отправки/получения данных.
- 3) Адрес, на который нужно отправлять запросы. Указан в данной документации ниже, но рекомендуется получать его у REX400.
- 4) ПО для подписи запросов: СКЗИ Верба OW, дискета с ключами для подписи запросов, утилита SCSIGNEX, архиватор ARJ. Подробнее см. [Приложение D, «Требуемое ПО и ключи»](#).

После получения перечисленных компонентов можно начинать настройку Credit Registry.

Для этого необходимо:

1. Проверить, что версия Credit Registry не ниже 6.18.0, а версия SSLGate – не ниже 4.10.*.
Внимание! Данное условие является обязательным.
Если используются более ранние версии, то необходимо запросить у МТЦ последние версии Credit Registry и SSLGate.
2. В Credit Registry на странице «Администрирование» указать «Регистрационный номер кредитной организации (ЦБ-ЦККИ)» (при помощи кнопки «добавить» в блоке «Рег. Номер кред. организации»). Получается у ЦБ.

Примечание. Если на странице «Администрирование» нет соответствующего блока, необходимо предоставить администратору в настройках роли право «Редактирование РНКО (ЦБ-ЦККИ)».

3. Создать и настроить профиль коннектора ЦБ-ЦККИ.

Добавление профиля коннектора

Коннектор:

Название профиля:

Описание профиля:

Приоритет профиля:

Максимальное количество запросов в пакете:

Максимальный интервал ожидания заполнения пакета: мин

Использовать тестовый режим запросов ЦККИ

Не использовать SSLGate (для криптографии и архивации)

Использовать SSLGate (для SMTP/SSL и POP3/SSL)

Настройки отправки почты (SMTP)

Email адрес АС ЦККИ:

Email адрес ("От кого"):

Адрес сервера:

Имя пользователя:

Пароль:

Настройки получения почты

Протокол: POP3 IMAP

Адрес сервера:

Имя пользователя:

Пароль:

Настройки telnet соединения

Использовать telnet соединение

Адрес:

Порт:

Логин пользователя:

Пароль пользователя:

Настройки кэша

Глубина используемого кэша:

Установить запрет на отключение кэша

Рис. 43

Параметр	Рекомендации
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большем числу соответствует больший приоритет.
Максимальное количество запросов в пакете	См. раздел "Пакетирование запросов ЦККИ" в данной документации.
Максимальный интервал ожидания заполнения пакета (в мин.)	
Использовать тестовый режим запросов ЦККИ	Для тестовых запросов в ЦККИ. К имени файла будет добавлено слово test и запрос будет направлен на стенд АС ЦККИ, содержащий тестовые данные.
Использовать SSLGate (для SMTP/SSL и POP3/SSL)	Стандартный вариант - протоколы SMTP/POP3, т.е. галочка не ставится. Если галочка не установлена, отправка и получение почты происходит по протоколам SMTP (по умолчанию используется порт 25) и POP3 (по умолчанию используется порт 110). Если галочка стоит, отправка и получение будут идти по протоколам SMTPs (по умолчанию используется порт 465) и POP3s (по умолчанию используется порт 995). Примечание. Если данная опция выставлена, и в администрировании, редактировании параметров указан прокси-сервер, то подключение к почтовому ящику будет идти через прокси-сервер.
Не использовать SSLGate (для криптографии и архивации)	Для данного типа настройки галочка стоять не должна , т.е. шифрование и архивация должны осуществляться с помощью Credit Registry.
Настройки отправки почты (SMTP)	
Email адрес АС ЦККИ	вводится одной строкой без пробелов: <a @rex400.ru"="" href="mailto:/%C=RU/A=INFOMAIL/P=MMBGUCBRF/O=GUCBRF/OU=POST/OU2=OTCHET/S=CKKI/G=OTCHET/">"/C=RU/A=INFOMAIL/P=MMBGUCBRF/O=GUCBRF/OU=POST/OU2=OTCHET/S=CKKI/G=OTCHET/"@rex400.ru
Email адрес "От кого"	<имя ПЯ из заявки>@rex400.ru
Адрес сервера исходящей почты (SMTP)	rex400.ru формат адреса – либо host, либо host:port. По умолчанию используется порт 25 (либо 465 при выставленном флаге - использовать SSLGate для SMTP ssl и POP3 ssl)
Имя пользователя (для подключения к серверу исходящей почты (SMTP))	<имя ПЯ из заявки>
Пароль (для подключения к серверу исходящей почты (SMTP))	<пароль из заявки>

Параметр	Рекомендации
Настройки получения почты	
Протокол (получения почты от АС ЦККИ)	POP3/IMAP
Адрес сервера (входящей почты)	rex400.ru формат адреса – либо host, либо host:port. По умолчанию используется порт 110 (либо 995 при выставленном флаге - использовать SSLGate для SMTP ssl и POP3 ssl)
Имя пользователя (для подключения к серверу входящей почты)	<имя ПЯ из заявки>
Пароль (для подключения к серверу входящей почты)	<пароль из заявки>
Настройки telnet соединения	
Использовать telnet соединение	галочка должна быть НЕ выставлена (для данного способа подключения).
Адрес telnet соединения	не используется для данного способа подключения
Порт telnet соединения	не используется для данного способа подключения
Логин пользователя	не используется для данного способа подключения
Пароль пользователя	не используется для данного способа подключения
Глубина используемого кэша	Задается в днях. Перед запросом в ЦККИ Credit Registry просматривает историю запросов. Если такой же запрос повторялся на протяжении последних <глубина кэша> дней, то ответ вернется из кэша. Использование кэша позволяет экономить на часто повторяющихся запросах.
Установить запрет на отключение кэша	Если галочка выставлена, пользователи не смогут делать запросы без использования кэша

4. В общих параметрах Credit Registry («Администрирование» -> «Параметры» -> «Основные параметры» -> Коннекторы -> «ЦККИ») заполнить поле «Период сканирования ответов (в минутах)».
5. Credit Registry с указанным периодом будет подключаться к почтовому серверу и проверять, пришел ли ответ на запрос.
6. Открыть порты для подключения к почтовому серверу.
7. Должен быть открыт доступ к адресу rex400.ru по портам 25 и 110 (без SSL) или 465 и 995 (подключение по SSL). В случае использования SSLGate подключение к почтовому серверу идет от SSLGate. Т.е. если SSLGate установлен на отдельной машине, доступ до почтового сервера должен открываться с машины с SSLGate.
8. Выполнить настройку SSLGate в соответствии с [приложением D](#).

9. Через права роли предоставить пользователям доступ к коннектору для работы с запросами ЦККИ.

10. Зайти на закладку ЦБ ЦККИ, сделать запрос.

Дополнение: Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение Б. Типичные ошибки настройки коннекторов** (стр. 132).

11.2 Настройка запросов ЦККИ через систему СВК

Необходимая информация и компоненты:

- 1) информационное письмо ЦБ, содержащее регистрационный номер кредитной организации, присвоенный банку.
- 2) Договор с ЦБ о запросах ЦККИ через систему СВК. В нем должны быть указаны IP адреса почтовых серверов, IP адрес, логин/пароль для подключения к этим серверам, а также адрес, на который нужно открывать telnet-сессию для открытия канала. Необходимо также открыть доступ в систему СВК. Подробнее см. ниже.
- 3) ПО для подписи запросов: СКЗИ Верба OW, дискета с ключами для подписи запросов, утилита SCSIGNEX, архиватор ARJ. Подробнее см. [приложение D, «Требуемое ПО и ключи»](#).

После получения перечисленных компонентов можно начинать настройку Credit Registry.

Для этого необходимо:

- 1) Открыть доступ в систему СВК. Данный пункт осуществляется банком **совместно с техническими специалистами ЦБ**.

Если доступ открыт, команда: telnet 192.168.19.20

вернет какое-либо приглашение (login authentication или logout authentication)

(адрес для открытия telnet-сессии получается у ЦБ)

Проверить, что версия Credit Registry не ниже 6.18.0, а версия SSLGate – не ниже 4.10.*.

***Внимание!** Данное условие является обязательным.

Если версии старше указанных, необходимо запросить у МТЦ последние версии Credit Registry и SSLGate.

- 2) В программе Credit Registry на странице [«Администрирование»](#) указать Регистрационный номер кредитной организации (ЦБ-ЦККИ) в блоке [«Рег. номер кред. организации»](#). Получается у ЦБ.

Примечание. Если на странице [«Администрирование»](#) нет соответствующего блока, необходимо предоставить администратору в настройках роли право [«РНКО \(ЦБ-ЦККИ\)»](#).

3) Создать и настроить профиль коннектора ЦБ-ЦККИ.

Параметр	Рекомендации
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большому числу соответствует больший приоритет.
Максимальное количество запросов в пакете	См. раздел 11.6 «Пакетирование запросов ЦККИ» в данной документации.
Максимальный интервал ожидания заполнения пакета (в мин.)	
Использовать тестовый режим запросов ЦККИ	Для тестовых запросов в ЦККИ. К имени файла будет добавлено слово test и запрос будет направлен на стенд АС ЦККИ, содержащий тестовые данные.
Использовать SSLGate (для SMTP/SSL и POP3/SSL)	Для данного способа подключения галочка стоять не должна , т.е. отправка и получение почты осуществляется по протоколам SMTP/POP3, а не SMTPs/POP3s
Не использовать SSLGate (для криптографии и архивации)	Для данного типа настройки галочка стоять не должна , т.е. шифрование и архивация должны осуществляться с помощью комплекса Credit Registry + SSLGate + SCSIGNEX.
Email адрес АС ЦККИ	ckki@ext-gate.svk.mskgtu.cbr.ru адрес актуален на момент написания документации (сентябрь 2011) рекомендуется брать из договора с ЦБ
Email адрес для указания в поле "От кого"	<имя пользователя>@svk.mskgtu.cbr.ru Имя пользователя для подключения есть в договоре с ЦБ
Адрес сервера исходящей почты (SMTP)	192.168.19.3 формат адреса – либо host, либо host:port. По умолчанию используется порт 25 Адрес актуален на момент написания документации. Рекомендуется брать из договора с ЦБ
Имя пользователя для подключения к серверу исходящей почты (SMTP)	Есть в договоре с ЦБ.
Пароль для подключения к серверу исходящей почты (SMTP)	Пароль. Есть в договоре с ЦБ
Протокол получения почты от АС ЦККИ	POP3
Адрес сервера входящей почты	192.168.19.4

Параметр	Рекомендации
	<p>формат адреса – либо host, либо host:port. По умолчанию используется порт 110</p> <p>Адрес актуален на момент написания документации.</p> <p>Рекомендуется брать из договора с ЦБ</p>
Имя пользователя для подключения к серверу входящей почты	Есть в договоре с ЦБ.
Пароль для подключения к серверу входящей почты	Есть в договоре с ЦБ.
Использовать telnet соединение	<p>Галочка должна быть выставлена.</p> <p>На момент запроса и проверки почты открывается telnet-соединение на указанный адрес. На приглашение LOGIN authentication вводятся логин/пароль, указанные в настройках ниже.</p> <p>Если в ответ приходит приглашение LOGOUT authentication (а не LOGIN authentication), то логин/пароль не вводятся.</p>
Адрес telnet соединения	<p>192.168.19.20</p> <p>Адрес актуален на момент написания документации.</p> <p>Рекомендуется брать из договора с ЦБ</p>
Порт telnet соединения	23
Логин пользователя	Есть в договоре с ЦБ.
Пароль пользователя	Есть в договоре с ЦБ.
Глубина используемого кэша	<p>Задается в днях.</p> <p>Перед запросом в ЦККИ Credit Registry просматривает историю запросов. Если такой же запрос повторялся на протяжении последних <глубина кэша> дней, то ответ вернется из кэша.</p> <p>Использование кэша позволяет экономить на часто повторяющихся запросах.</p>
Установить запрет на отключение кэша	Если галочка выставлена, пользователи не смогут делать запросы без использования кэша.

- 4) В общих параметрах Credit Registry («Администрирование» -> «Параметры» -> «Основные параметры» -> Коннекторы -> «ЦККИ») заполнить поле «Период сканирования ответов (в минутах)».
- 5) Credit Registry с указанным периодом будет подключаться к почтовому серверу и проверять, пришел ли ответ на запрос.
- 6) Выполнить настройку SSLGate в соответствии с [приложением D](#).
- 7) Через права роли предоставить пользователям доступ к коннектору для работы с запросами ЦККИ.
- 8) Зайти на закладку ЦБ ЦККИ, сделать запрос.

Дополнение: Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение Б. Типичные ошибки настройки коннекторов** (стр. 132).

11.3 Настройка запросов ЦККИ через каталоги отправки банковской отчетности (подписание и шифрование осуществляется внешним ПО, в частности, ПТК ПСД)

Необходимая информация и компоненты:

- 1) информационное письмо ЦБ, содержащее регистрационный номер кредитной организации, присвоенный банку.
- 2) Каталог для отправки запросов и каталог для получения ответов.

При данном способе настройки подписание, шифрование и отправка осуществляются внешним ПО, настраиваемым сотрудниками банка (подразумеваемое ПО, осуществляющее подписание, шифрование и отправку - ПТК ПСД).

Подразумеваемый вариант - использовать каталоги, используемые для отправки банковской отчетности в ЦБ.

Настройка Credit Registry в данном случае заключается в следующем:

- 1) В программе Credit Registry на странице «Администрирование» указать Регистрационный номер кредитной организации (ЦБ-ЦККИ) в блоке «Рег. номер кред. организации». Получается у ЦБ.

Примечание. Если на странице «Администрирование» нет соответствующего блока, необходимо предоставить администратору в настройках роли право «РНК (ЦБ-ЦККИ)».

- 2) Создать и настроить профиль коннектора ЦБ-ЦККИ.

Параметр	Рекомендации
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большому числу соответствует больший приоритет.
Максимальное количество запросов в пакете	См. раздел 11.6 «Пакетирование запросов ЦККИ» в данной документации.
Максимальный интервал ожидания заполнения пакета (в мин.)	
Использовать тестовый режим запросов ЦККИ	Для тестовых запросов в ЦККИ. К имени файла будет добавлено слово test и запрос будет направлен на стенд АС ЦККИ, содержащий тестовые данные.

Параметр	Рекомендации
Использовать SSLGate (для SMTP/SSL и POP3/SSL)	Для данного способа подключения галочка стоять не должна , т.е. отправка и получение почты осуществляется по протоколам SMTP/POP3, а не SMTPs/POP3s
Не использовать SSLGate (для криптографии и архивации)	Для данного типа настройки галочка должна быть выставлена , т.е. шифрование и архивация осуществляются не с помощью Credit Registry
Остальные параметры	Не заполняются для данного типа подключения

3) Заполнить параметры коннектора ЦККИ (закладка «Администрирование» -> «Параметры» -> «Основные параметры» -> Коннекторы -> «ЦККИ»):

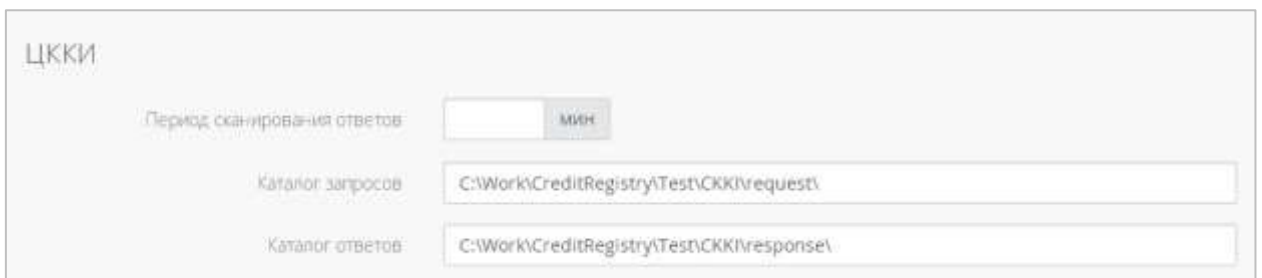


Рис. 44 Настройки коннектора ЦККИ в основных параметрах системы

Период сканирования ответов от АС ЦККИ (в минутах)	Целое число. Раз в указанное количество минут Credit Registry будет проверять каталог ответов на наличие там xml-файлов
Каталог запросов	В этот каталог будут выкладываться xml-запросы (не подписанные, не зашифрованные)
Каталог ответов	Из этого каталога забираются xml-файлы с названием вида K04_XXXX_XXXXXXXXXXXXXXXXXXXXXXXXX_ckki.xml Остальные файлы не затрагиваются.

Примечание. Использование сетевых каталогов возможно, но для этого необходимо проверить, что к этим папкам есть доступ под учетной записью этого компьютера (доступ на чтение, запись, удаление).

- 4) Через права роли предоставить пользователям доступ к коннектору для работы с запросами ЦККИ.
- 5) Зайти на закладку ЦБ ЦККИ, сделать запрос.

Дополнение: Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение Г. Типичные ошибки настройки коннекторов** (стр. 132).

11.4 Настройка запросов ЦККИ через каталоги запросов и ответов (подписание и шифрование осуществляется комплексом CRE + SSLGate + SCIGNEX + VerbaOW)

Необходимая информация и компоненты:

- 1) информационное письмо ЦБ, содержащее регистрационный номер кредитной организации, присвоенный банку.
- 2) Каталог для отправки запросов и каталог для получения ответов.

При данном способе настройки отправка осуществляются внешним ПО, настраиваемым сотрудниками банка. Подразумеваемое ПО для отправки – УТА (универсальный транспортный адаптер).

Настройка Credit Registry в данном случае заключается в следующем:

- 1) В программе Credit Registry на странице «Администрирование» указать Регистрационный номер кредитной организации (ЦБ-ЦККИ) в блоке «Рег. номер кред. организации». Получается у ЦБ.

Примечание. Если на странице «Администрирование» нет соответствующего блока, необходимо предоставить администратору в настройках роли право «РНКО (ЦБ-ЦККИ)».

- 2) Создать профиль коннектора ЦБ-ЦККИ.

Параметр	Рекомендации
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большем числу соответствует больший приоритет.
Максимальное количество запросов в пакете	См. раздел 11.6 «Пакетирование запросов ЦККИ» в данной документации.
Максимальный интервал ожидания заполнения пакета (в мин.)	
Использовать тестовый режим запросов ЦККИ	Для тестовых запросов в ЦККИ. К имени файла будет добавлено слово test и запрос будет направлен на стенд АС ЦККИ, содержащий тестовые данные.
Использовать SSLGate (для SMTP/SSL и POP3/SSL)	Для данного способа подключения галочка стоять не должна

Параметр	Рекомендации
Не использовать SSLGate (для криптографии и архивации)	Для данного типа настройки галочка стоять не должна , т.е. шифрование и архивация осуществляются с помощью Credit Registry
Остальные параметры	Не заполняются для данного типа подключения

3) Заполнить параметры коннектора ЦККИ (закладка «Администрирование» -> «Параметры» -> «Основные параметры» -> Коннекторы -> «ЦККИ»):

Рис. 45 Настройки коннектора ЦККИ в основных параметрах системы

период сканирования ответов от АС ЦККИ (в минутах)	Целое число. Раз в указанное количество минут Credit Registry будет проверять каталог ответов на наличие там файлов-ответов.
каталог запросов	В этот каталог будут выкладываться xml-запросы (подписанные, зашифрованные и заархивированные)
каталог ответов	Из этого каталога забираются файлы с названием вида СККИ.XML* - обрабатываются как ответы ЦККИ (подписанные, зашифрованные и заархивированные) receipt.xml* - подтверждения от МГТУ о получении запроса, обрабатываются. *.kvt0 - подтверждения от ЦККИ о получении запроса, удаляются. *.kvt1 - сообщения от ЦККИ о том, что сообщение не принято, удаляются, содержание пишется в лог stdout. Статус запроса не меняется, т.к. по файлу *.kvt1 невозможно однозначно определить, на какое сообщение пришел ответ. Остальные файлы не затрагиваются.

Примечание. Использование сетевых каталогов возможно, но для этого необходимо проверить, что к этим папкам есть доступ под учетной записью этого компьютера (доступ на чтение, запись, удаление).

- 4) Через права роли предоставить пользователям доступ к коннектору для работы с запросами ЦККИ.
- 5) Зайти на закладку ЦБ ЦККИ, сделать запрос.

Дополнение: Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение Б. Типичные ошибки настройки коннекторов** (стр. 132).

11.5 Настройка запросов ЦККИ через НБКИ

Примечание: Если у вас уже есть настроенный и работающий коннектор (для одного из сервисов ФМС, ФМС2, ГИБДД, ТСЗ, БРС, ЦККИ через НБКИ), и вам нужно настроить другой коннектор из этого списка, то код участника, логин, пароль и сертификат можно скопировать из уже настроенного. Это относится только к ЛИЧНОМУ сертификату. Сертификат НБКИ нужно будет устанавливать в любом случае.

Необходимо выполнить такие действия:

1. На машине с SSLGate установить личный сертификат в сертификаты локального компьютера, следуя инструкции Приложения А. (Личный и корневой сертификаты получают в НБКИ).
2. На машине с SSLGate установить в личные сертификаты локального компьютера сертификат «СГКО НБКИ – YYYY», где YYYY – год выпуска сертификата (например: «СГКО НБКИ - 2017»). Установка сертификата бюро аналогична установке сертификата удостоверяющего центра - делается импорт в **личные** сертификаты в консоли mmc. Это можно сделать аналогично установке сертификата удостоверяющего центра (см. [«ПРИЛОЖЕНИЕ А»](#)).
3. Войти в систему Credit Registry и добавить серийный номер личного сертификата и серийный номер сертификата СГКО НБКИ в «Справочник сертификатов» (см. «Руководство пользователя Credit Registry»).

На закладке **«Администрирование»** найти раздел **«Сертификаты»** и воспользоваться кнопкой **«добавить»** в правом верхнем углу таблицы. Впоследствии введенный номер сертификата необходимо указывать в настройках коннектора.

4. Настроить параметры коннектора ЦККИ через НБКИ

После добавления нового коннектора устанавливаются следующие параметры:

Параметр	Рекомендации
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большому числу соответствует больший приоритет.

Параметр	Рекомендации
Код участника, Имя и Пароль	Информация предоставляется сотрудниками НБКИ.
Использовать SSLGate (для SMTP/SSL и POP3/SSL)	Стандартный вариант - протоколы SMTP/POP3, т.е. галочка не ставится. Если галочка не установлена, отправка и получение почты происходит по протоколам SMTP (по умолчанию используется порт 25) и POP3 (по умолчанию используется порт 110). Если галочка стоит, отправка и получение будут идти по протоколам SMTPs (по умолчанию используется порт 465) и POP3s (по умолчанию используется порт 995).
Email для НБКИ	CCCH@nbki.ru , тестового адреса нет.
Email адрес для указания в поле «От кого»	Данные предоставляются системным администратором банка.
Адрес сервера исходящей почты (SMTP)	Примечание: формат адреса – либо host, либо host:port. По умолчанию используется порт 25.
Имя пользователя для подключения к серверу исходящей почты (SMTP)	
Пароль для подключения к серверу к серверу исходящей почты (SMTP)	
Протокол получения почты от АС ЦККИ	Обычно POP3
Адрес сервера входящей почты	Данные предоставляются системным администратором банка. Примечание: формат адреса – либо host, либо host:port. По умолчанию используется порт 110.
Имя пользователя для подключения к серверу входящей почты	
Пароль пользователя для подключения к серверу входящей почты	
Серийный номер личного сертификата от НБКИ	Личный сертификат получается в НБКИ.
Серийный номер личного сертификата бюро НБКИ	«СГКО НБКИ - YYYY» (где YYYY – год выпуска сертификата, например: «СГКО НБКИ - 2017») Предоставляется менеджером НБКИ.

- В основных параметрах Credit Registry («Администрирование» -> «Параметры» -> «Основные параметры» -> «ЦККИ») заполнить поле «Период сканирования ответов (в минутах)».
- Добавить права на коннектор в ролях тех пользователей, которые будут отправлять запросы в ЦККИ.

7. Зайти на закладку «ЦККИ через НБКИ», сделать запрос.

Примечание: необходимо согласовать с менеджером НБКИ имя пользователя, сертификат и почтовый адрес, с которыми будут осуществляться запросы.

Дополнение: Список типичных ошибок настройки коннекторов приведен в данной документации: **Приложение Г. Типичные ошибки настройки коннекторов** (стр. 132).

11.6 Пакетирование запросов ЦККИ

Для снижения нагрузки на сервер на стороне ЦБ все запросы ЦККИ отправляются пакетно.

Введены два параметра:

- Максимальное количество запросов в пакете
- Максимальный интервал ожидания заполнения пакета (в мин.)

Каждый запрос сначала переходит в статус "на отправку". В статус "в процессе выполнения" запрос переходит после отправки пакета.

Отправка пакета запросов происходит при выполнении одного из условий - достигнуто максимальное количество запросов в режиме "на отправку", либо прошло заданное время с начала формирования пакета заявок.

При количестве запросов менее 500 запросов ЦККИ в сутки мы рекомендуем заполнять параметр "максимальное количество запросов в пакете" значением 1, тогда каждый пакет будет содержать только один запрос и отправляться сразу же, без ожидания новых запросов.

В случае, если банк делает больше 500 запросов ЦККИ в сутки, рекомендуем заполнять данные параметры значениями - 1 мин и 5 запросов, либо большими значениями, если от ЦБ поступит такая рекомендация.

12 Настройка коннектора СМЭВ ФМС

Внимание: для успешного взаимодействия с ФМС через СМЭВ на машине с SSLGate необходимо установить КриптоПро .NET (<http://www.cryptopro.ru/products/net>). Данный продукт используется для работы с XML-подписями, которые применяются согласно форматам СМЭВ.

Ниже представлен список действий, которые необходимо выполнить администратору системы для настройки коннектора:

- 1) Добавить новый коннектор:
 - Зайти в CRE под пользователем с правами администратора, по ссылке «Администрирование» перейти в соответствующий раздел, далее в секции «Профили коннекторов» нажать на кнопку «Добавить»:



Рис. 46 Кнопка «добавить» в секции «Профили коннекторов»

- Далее откроется окно «Добавление профиля коннектора», где необходимо указать следующие параметры (параметры, выделенные жирным шрифтом, обязательны к заполнению)

Рис. 47 Добавления профиля коннектора СМЭВ ФМС

Параметр	Рекомендации
Приоритет профиля коннектора	Число, должно быть уникальным для каждого профиля. Большому числу соответствует больший приоритет.
Адрес сервиса	Для тестового доступа http://smev-mvf.test.gosuslugi.ru:7777/gateway/services/SID0003110 Для «боевого» доступа http://172.16.90.14:7777/gateway/services/SID0003418 (адрес доступен через защищенное соединение, установленное со СМЭВ через ViPNet Coordinator HW100/HW1000)

Сертификат	Личный сертификат, выпущенный в одном из аккредитованных удостоверяющих центров. Перечень центров доступен по адресу http://minsvyaz.ru/ru/directions/?regulator=118 Сертификат выбирается из списка, который также представляет собой «Справочник личных сертификатов». Порядок установки личного сертификата см. в « ПРИЛОЖЕНИЕ А ».
Настройки кэша	
Глубина используемого кэша	Задается в днях
Настройки соединения с сервисом	
Время ожидания ответа БКИ (сек)	Рекомендуемое значение – 60
Максимальное количество подключений к БКИ	Рекомендуемое значение – 20
Максимальное время ожидания в очереди (сек)	Рекомендуемое значение – 60
Максимальное время формирования ЭЦП (сек)	Рекомендуемое значение – 60

- После указания параметров нажать «**Сохранить**».
- 2) Настроить общесистемные параметры для взаимодействия со СМЭВ ФМС:
- Перейти в «Администрирование» -> «Параметры» -> «Основные параметры» -> «СМЭВ ФМС». Указать следующие настройки (все параметры обязательны к заполнению)

СМЭВ ФМС

Тип сообщения	<input type="text" value="GSRV"/>
Код системы банка	<input type="text" value="123456"/>
Название системы банка	<input type="text" value="ОАО Банк"/>
Код запрашивающей организации	<input type="text" value="0000000001"/>
Код пользователя	<input type="text" value="987654"/>
Фамилия пользователя	<input type="text" value="Иванов"/>
Имя пользователя	<input type="text" value="Иван"/>
Отчество пользователя	<input type="text" value="Иванович"/>

Рис. 48 Параметры СМЭВ ФМС

Параметр	Описание
Тип сообщения	Выбор типа сообщения из выпадающего списка
Код системы банка	состоит из 9 знаков (первые шесть – код банка); значение попадает в <code>//Message/Sender/Code</code>

Название системы банка	значение попадает в <code>//Message/Sender/Name</code>
Код запрашивающей организации	назначается ФМС; значение попадает в <code>//MessageData/AppData/user/organization</code>
Код пользователя	значение попадает в <code>//MessageData/AppData/user/person/id</code>
Фамилия пользователя	значение попадает в <code>//MessageData/AppData/user/person/lastName</code>
Имя пользователя	значение попадает в <code>//MessageData/AppData/user/person/firstName</code>
Отчество пользователя	значение попадает в <code>//MessageData/AppData/user/person/secondName</code>

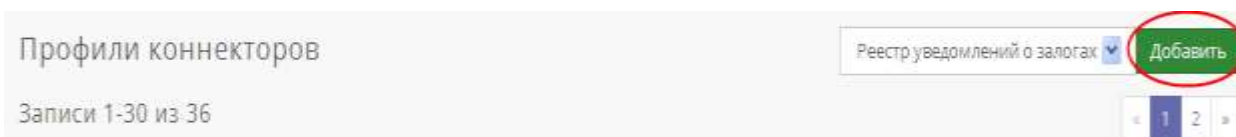
После ввода всех параметров нажать **«Сохранить»**.

13 Настройка коннектора Реестр залогов и уведомлений

Для обеспечения корректной работы коннектора “Реестр залогов и уведомлений” необходимо предварительно произвести следующую последовательность действий:

Примечание: Для пользователей API нотариуса Амелькиной Е.А необходимо зарегистрироваться на сайте <http://amelkina.ru/>. После регистрации необходимо в личном кабинете добавить сертификат электронной подписи с включенной опцией авторизации и в разделе «Профиль пользователя» заполнить подразделы «Данные организации» и «Данные представителя». Следует отметить, что данные, указанные в этих разделах, должны совпадать с данными в сертификате электронной подписи.

1. Добавить сертификат нотариуса и сертификат электронной подписи залогодателя в систему CreditRegistry.
 - На машине с SSLGate установить сертификат нотариуса и сертификат электронной подписи в хранилище сертификатов локальной машины (согласно Приложению А).
 - Добавить серийный номер сертификата нотариуса и сертификата электронной подписи залогодателя в «Справочник сертификатов». Для этого необходимо: войти в систему Credit Registry с правами администратора, на закладке «Администрирование» найти раздел «Сертификаты», воспользоваться кнопкой «Обновить» в правом верхнем углу таблицы – это приведет к импорту информации о сертификатах с машины, на которой развернут SSLGate.
2. Добавить профиль коннектора “Реестр залогов и уведомлений”:
 - Войти в систему Credit Registry с правами администратора, по ссылке «Администрирование» перейти в соответствующий раздел, далее в секции «Профили коннекторов» нажать на кнопку «Добавить»:



- Далее, откроется окно «Добавление профиля коннектора», где необходимо заполнить форму, состоящую из нескольких разделов (параметры, выделенные жирным шрифтом, обязательны к заполнению). Рассмотрим основные настройки.

Редактирование профиля коннектора

Коннектор:

Название профиля:

Описание профиля:

Приоритет профиля:

Адрес сервиса:

Код разработчика:

Настройки сертификатов шифрования

Номер сертификата нотариуса:

Номер сертификата цифровой подписи:

Профиль нотариуса

ФИО нотариуса:

Нотариальный округ получателя уведомления:


Параметр	Рекомендации
Приоритет профиля коннектора	Большем числу соответствует больший приоритет профиля коннектора
Адрес сервиса	Для подключения к API нотариуса Амелькиной Е.А. ввести http://amelkina.ru/api.php/
Код разработчика	Уникальный пароль для доступа к API нотариуса. Выдается службой поддержки API нотариуса индивидуально для каждого залогодателя
Номер сертификата нотариуса	Открытая часть сертификата шифрования, которая выдается нотариусом. Для пользователей API Амелькиной Е.А сертификат можно загрузить на сайте http://amelkina.ru/
Номер сертификата цифровой подписи	Номер сертификата электронной подписи залогодателя для подписи уведомления о залоге. Подпись должна быть выдана квалифицированным удостоверяющим центром.
ФИО нотариуса	Фамилия и инициалы нотариуса, к API которого производится подключение
Нотариальный округ получателя уведомления	Название округа, где расположен залогодатель. Указывается в родительном падеже.

- Разделы «Описание организации залогодержателя» и «Адрес организации залогодержателя» заполняются данными об организации залогодержателе (о банке)
- В разделах «Данные по представителю залогодержателя» и «Адрес представителя залогодержателя» должна быть указана информация о представителе залогодержателя

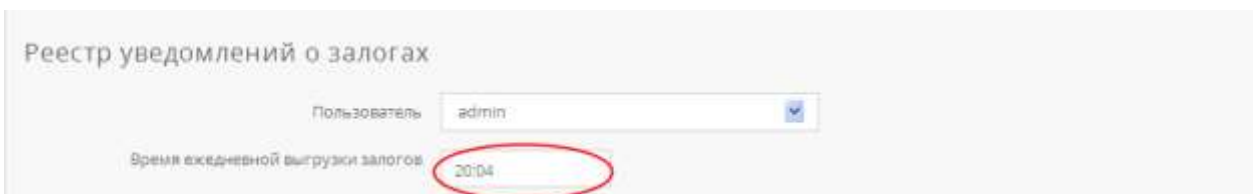
Описание организации залогодержателя

Название организации	<input type="text" value="БМВ Банк"/>
ОГРН организации	<input type="text" value="1085000001998"/>
ИНН организации	<input type="text" value="5047093433"/>
Контактный email организации	<input type="text" value="somewhere@gmail.com"/>


Адрес организации залогодержателя

Регион	<input type="text" value="Москва г."/> 
Округ	<input type="text" value="Москва"/>
Город	<input type="text"/>
Местоположение	<input type="text"/>
Улица	<input type="text" value="Горчакова"/>
Номер дома	<input type="text" value="4"/>

3. Настроить работу расписания ежедневной выгрузки залогов в параметрах коннектора:
- Войти в систему Credit Registry с правами администратора, по ссылке [«Администрирование»](#) перейти в соответствующий раздел. Далее, последовательно выбрать следующие пункты [«Параметры»](#) -> [«Основные параметры»](#) -> [Коннекторы](#) -> [«Реестр уведомлений о залогах»](#)
 - Из всплывающего списка необходимо выбрать пользователя, от чьего имени будет запускаться автоматическая выгрузка залогов. Необходимо, чтобы пользователь обладал правами доступа к коннектору “Реестр залогов и уведомлений”.
 - В поле [«Время ежедневной выгрузки залогов»](#) следует указать время старта выгрузки залогов в формате *чч:мм* (пример: 20:04). Без заполнения этого поля выгрузка залогов невозможна.



Реестр уведомлений о залогах

Пользователь	<input type="text" value="admin"/> 
Время ежедневной выгрузки залогов	<input type="text" value="20:04"/>

14 Настройка прокси-соединения для связи сервера Credit Registry с БКИ (НБКИ, ОКБ, БРС)

Credit Registry корректно работает со следующими вариантами прокси-соединения:

- а) прокси-сервер не используется;
- б) http прокси-сервер с BASIC авторизацией;
- в) http прокси-сервер без авторизации.

Обращаем особое внимание, что Credit Registry не поддерживает NTLM или доменную (Negotiate) авторизацию. Допускается использовать аутентификацию без запроса логина/пароля по IP адресу сервера Credit Registry.

Для установки прокси-соединения в настройках Credit Registry необходимо прописать тип, адрес и порт прокси-сервера, логин, пароль. Для этого пользователь с правами администратора заходит на страницу «Администрирование» -> «Параметры» -> «Основные параметры» -> «Настройки прокси» и заполняет блок параметров.

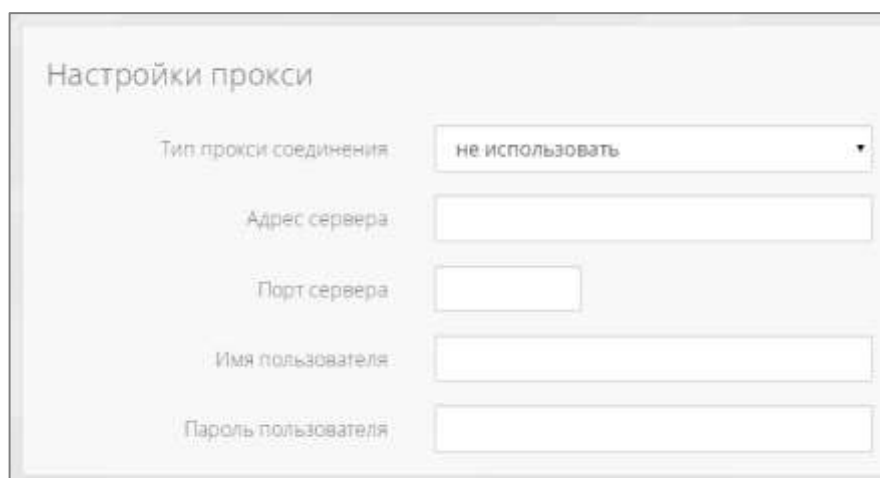


Рис. 49 Блок параметров для настройки прокси

Также следует указать наличие прокси-сервера в настройках SSL-шлюзов: страница «Администрирование» -> раздел «Список SSL-шлюзов» -> кнопка «**добавить**» -> форма добавления SSL-шлюза.

Рис. 50 Список SSL шлюзов

Рис. 51 Добавление/редактирование SSL шлюза

Настройка самого прокси-сервера – целиком задача администраторов сети Банка!

Примечание. Использование прокси-сервера может быть включено/выключено только для всех коннекторов одновременно. Исключение составляют коннекторы ЦККИ, Equifax, Equifax агент и Equifax FPS. Для коннекторов Equifax/Equifax-агент/Equifax FPS прокси-сервер не используется никогда, для коннектора ЦККИ прокси-сервер используется только при включенной опции "Использовать SSLGate (для SMTP/SSL и POP3/SSL)".

15 Настройка потоковых запросов

Модуль потоковых запросов предназначен для выполнения запросов с использованием механизма БД с поддержкой запросов в следующие БКИ:

- НБКИ
- ЭКС (Equifax Credit Services)
- ОКБ (Experian-Interfax)
- БРС
- ФМС
- ГИБДД
- ЦККИ
- FPS
- NH

Используя этот механизм, внешняя интегрируемая система может выполнять запросы, помещая их данные в специальные таблицы. Ответы на запросы также помещаются Credit Registry

в другие таблицы после их выполнения. Функционал предназначен для получения КИ физических лиц.

Потоковые запросы работают следующим образом:

- 1) Внешняя система вносит данные запроса в таблицу **TCS_B2B_REQUEST**.

В случае выполнения группового запроса, внешняя система помещает в таблицу столько записей, сколько запросов к различным БКИ должно быть сделано (записи различаются полями **BKI_CODE** и, возможно, **SUB_REQUEST_CODE**). При этом поле **GROUP_UID** должно соответствовать пользовательскому идентификатору групповой кредитной заявки. Для всех записей, относящихся к одному групповому запросу, значение этого поля должно быть одинаковым. Внешняя система должна обеспечить уникальность идентификации кредитных заявок. Кроме того, все записи, относящиеся к одному групповому запросу (имеющие одинаковое значение **GROUP_UID**), должны помещаться в таблицу в рамках одной транзакции СУБД.

- 2) По команде «оператора запроса» («**оператор запроса**» – пользователь **Credit Registry Enterprise (CRE)** имеющий права для запросов кредитных историй НБКИ, команда – нажатие кнопки на страничке «**Потоковые запросы**») система CRE запускает определенное число потоков для исполнения запросов (поток запроса).

Число потоков настраивается администратором системы **Credit Registry** (рекомендуемое число 2 - 4). Данный параметр указывает, какое количество фоновых потоков операционной системы будет использоваться для обработки запросов.

- 3) После запуска поток запроса последовательно выбирает за таблицы **TCS_B2B_REQUEST** «необработанную» запись о субъекте и одновременно отмечает эту запись как обрабатываемую, выполняет запрос в указанный источник данных, записывает результат исполнения запроса в таблицу **TCS_B2B_RESPONSE**. Если данная операция выполняется в рамках группового запроса, в поле **TCS_B2B_RESPONSE.GROUP_UID** идентификатор группового запроса.

- 4) Если при помещении очередной записи в таблицу **TCS_B2B_RESPONSE** CRE фиксирует, что кол-во ответов, полученных по одному групповому запросу, соответствует кол-ву соответствующих записей в таблице запросов (т.е. ответы на все запросы к БКИ получены), запускается процедура унификации и сведения.

- 5) Если поток запроса больше не находит необработанных записей, он прекращает работу.

Описание таблиц **TCS_B2B_REQUEST** и **TCS_B2B_RESPONSE** находится в документе «Модуль потоковых запросов CRE».

Потоковые запросы к сервису НБКИ В2В могут выполняться с использованием дополнительного параметра, передаваемого в поле **SUB_REQUEST_CODE** таблицы **TCS_B2B_REQUEST**. Значение данного поля определяет внутренний дополнительный код для запросов со скорингом и без скоринга.

Примечание: перед использованием дополнительных кодов НБКИ убедитесь, что в настройках соответствующего профиля (используемого для потоковых запросов) заданы настройки подключения к соответствующим сервисам: URL стандартного или скорингового сервисов НБКИ в соответствии с используемым кодом:

- «не указано» - используется сервис по умолчанию в настройках профиля НБКИ;
- «1» - используется стандартный сервис НБКИ;
- «2» - используется скоринг-сервис НБКИ FICO;
- «3» - используется FICO Expansion Score;
- «5» - используется скоринг-сервис НБКИ FICO2;
- «7» - используется анти фрод скоринг НБКИ.

16 Настройка пакетных запросов

Модуль пакетных запросов предоставляет возможность отправки пакетных запросов по нескольким субъектам в различные БКИ для последующей обработки данных запросов и получения системой CRE ответов по ним.

Основным отличием от других способов (интерфейсов CRE) получения кредитных отчетов является именно **пакетный** режим работы (т.е. это не “онлайн” режим).

- *Преимущество:* при помощи пакетных запросов можно одновременно запросить в бюро информацию о большом количестве субъектов.
- *Недостаток:* обработка пакетных запросов на стороне бюро может занимать существенное время (вплоть до нескольких суток).

Данный модуль использует такой же интерфейс, что и модуль CRE «Потоковые запросы». Это упрощает процедуры интеграции на стороне банка: один и тот же интерфейс может быть использован для работы как в потоковом, так и в пакетном режиме.

Особенности пакетного режима (отличия от потокового):

- 1) Наполнение таблицы **TCS_B2B_REQUEST** для отправки пакетного запроса возможно в двух режимах:
 - a. Внешняя система помещает в таблицу **TCS_B2B_REQUEST** все записи, относящиеся к одному пакету, в рамках одной транзакции. При этом в поле **STATE** для всех записей указывается значение “0”.
 - b. Внешняя система помещает в таблицу **TCS_B2B_REQUEST** записи в рамках нескольких транзакций. При этом для записей пакета в поле **STATE** указывается значение “9” – это позволит предотвратить взятие пакета в обработку до окончания его формирования внешней системой. После того, как пакет будет

сформирован, т.е. все необходимые записи добавлены в таблицу, внешняя система выполняет (одной транзакцией) UPDATE: для всех записей пакета необходимо установить в поле STATE значение "0".

- 2) Признаком того, что записи составляют один пакет, является заполненное одинаковым значением (для одного пакета) поле BATCH_ID. Это поле определяет идентификатор пакета (записи с одинаковым значением BATCH_ID составляют один пакет). Если это поле не будет заполнено, то запись не будет обработана в пакетном режиме (произойдет попытка обработки в потоковом режиме).
- 3) Перечень БКИ, в которые требуется направить пакет, определяется полем CONNECTOR_CODES – список БКИ через запятую: 0 – НБКИ, 3 – ЭКС, 6 – ОКБ.
- 4) Поля BKI_CODE и GROUP_UID при работе в пакетном режиме не анализируются.

Ограничения:

- 1) Для всех записей одного пакета должен использоваться одинаковый перечень БКИ (поле CONNECTOR_CODES).
- 2) Внешняя система должна гарантировать заполнение PROSPECT_ID уникальными значениями для каждой записи в TCS_B2B_REQUEST. По значениям PROSPECT_ID будут идентифицироваться одиночные запросы в рамках пакета (CRE не будет проверять PROSPECT_ID на уникальность).
- 3) В ОКБ можно отправить только один пакет в сутки (это ограничение бюро).

После получения пакетного ответа из БКИ происходит его дробление на одиночные и обогащение ими кэша запросов CRE (сохранение одиночных запросов/ответов в таблицу CONNECTOR_DATA). Соответственно, данные одиночные отчеты становятся доступны пользователям CRE при помощи стандартного функционала просмотра [Истории запросов](#).

При настроенной "онлайн" выгрузке унифицированных отчетов («[Основные параметры](#)» - > секция «[Настройки подключения к Базам Данных для сохранения отчетов](#)» -> галка «[выгрузка в онлайн](#)») происходит их сохранение в SF-таблицы.

Особенности:

- 1) Полученные отчеты из разных бюро не сводятся, т.к. получение пакетных ответов из разных бюро происходит в разные моменты времени (которые могут быть сильно разнесены друг с другом) и асинхронно (что делает возможным ситуацию, когда из какого-то бюро пакетный ответ вообще не будет никогда получен).
- 2) Признаком того, что в одном из пришедших пакетных ответов присутствовала информация о запрошенном клиенте, является создаваемая CRE запись в таблице TCS_B2B_RESPONSE (описание таблицы см. в документе «Модуль потоковых запросов CRE»). Например, если клиент запрашивался в пакете, направленном в три бюро, то в TCS_B2B_RESPONSE может быть создано до трёх записей, относящихся к данному клиенту (по одной для каждого БКИ).
- 3) У записей в TCS_B2B_RESPONSE, относящихся к пакетным ответам, заполнение поля XML_CONTENT (содержимое ответа БКИ) не реализовано.

Описание таблиц, параметров модуля и другую дополнительную информацию см. в документации CRE «Модуль потоковых запросов» и «Модуль пакетных запросов».

17 Взаимодействие с IBM WebSphere MQ

Через очереди сообщений реализуется такое же взаимодействие, как и с web-сервисами CRE. Особенности:

1. Обмен построен на основе взаимодействия CRE с двумя очередями: входной и выходной. Связка сообщений производится стандартным образом по *CorrelationID* (у выходного сообщения устанавливается равным *MessageID* входного сообщения).
2. Формат сообщений: SOAP (как при вызове web-сервисов).
3. Для определения кодировки входящего сообщения CRE использует свойство *JMS_IBM_Character_Set* из заголовка MQ – поддерживаются следующие значения:
 - “1208” или “UTF8” (по умолчанию)
 - “1251”
4. Имя вызываемого сервиса определяется по свойству *CRE_SERVICE_NAME*. Если оно не задано, то используется значение по умолчанию: “ConnectorService”. Список доступных сервисов можно получить по ссылке http://cre_host:8080/credit_registry/xservices, где *cre_host* – имя машины, на которой развернута CRE в банке.
5. CRE поддерживает работу с двумя менеджерами очередей: основным и резервным (на каждом – своя входная и выходная очереди). Чтение обеих входных очередей осуществляется параллельно (синхронное взятие по одному сообщению) и независимо (на каждый менеджер очередей – свой servlet). Основной и резервный менеджеры очередей равноправны (нет разделения по приоритетам).
6. В случае останова сервера приложений максимальные потери сообщений могут достигать заданного в настройках CRE количества потоков + 2 (общее количество сообщений, взятых в обработку).
7. В случае возникновения какой-либо ошибки подключения к очереди MQ повторная попытка подключения осуществляется через указанный интервал в секундах (по умолчанию 60).
8. Если в течение одного часа очередь была пуста (не поступало ни одного сообщения), то осуществляется принудительное переподключение к очереди.
9. Каждые 100 мс – попытка взятия новых сообщений в обработку (проверка состояний потоков).

17.1 Предварительные условия

- IBM WebSphere MQ сконфигурирован для поддержки JMS-приложений
- На машине с CRE установлен WebSphere MQ client или имеется набор jar-библиотек от IBM для поддержки JMS

17.2 Настройка WebSphere MQ

17.2.1 Создание фабрики соединений

Открыть WebSphere MQ Explorer и выполнить следующие шаги:

1. Создать менеджер очередей: основной и резервный (если требуется). В момент создания менеджеров очередей также создать получателей запросов (listener).
2. Для каждого менеджера очередей создать 2 очереди: входную и выходную.
3. Создать канал соединения с сервером.

Примеры снимков экрана WebSphere MQ Explorer:

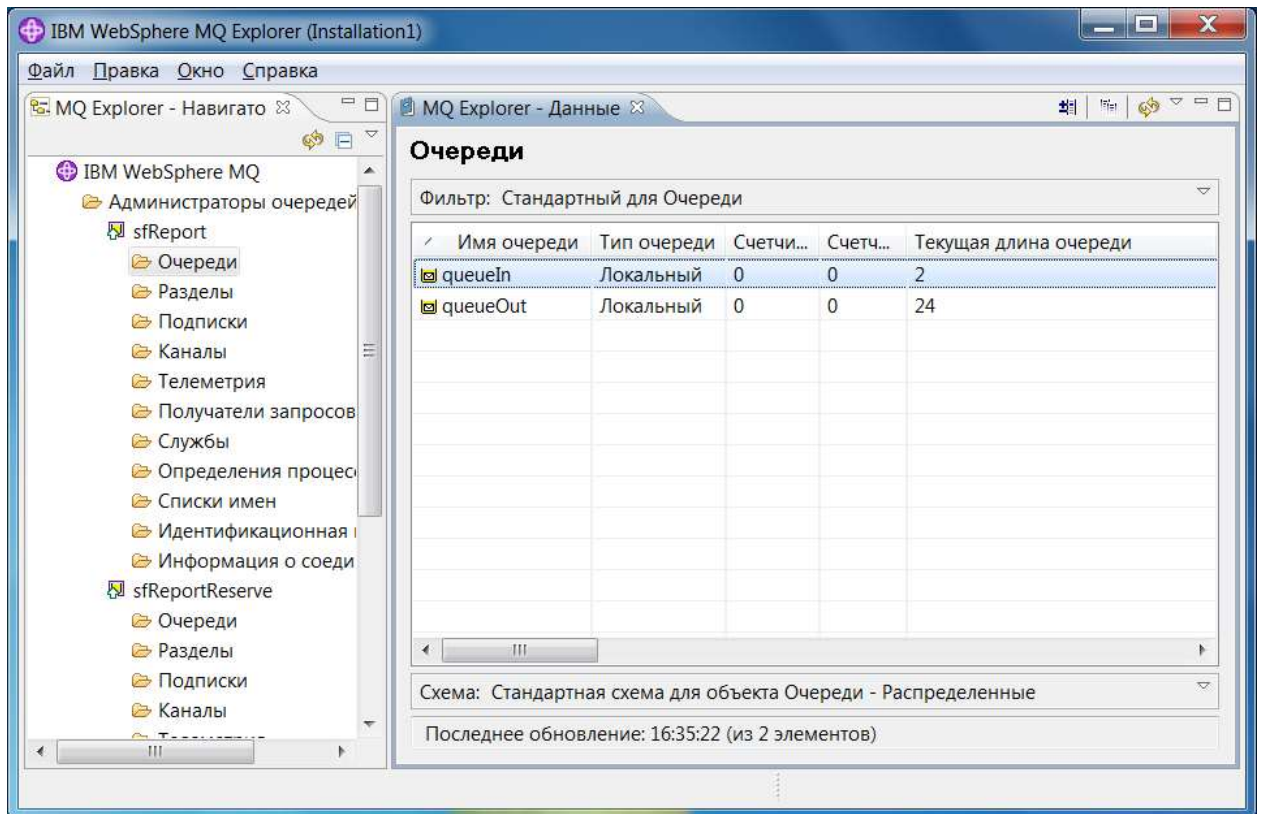


Рис. 52 Снимок экрана WebSphere MQ Explorer

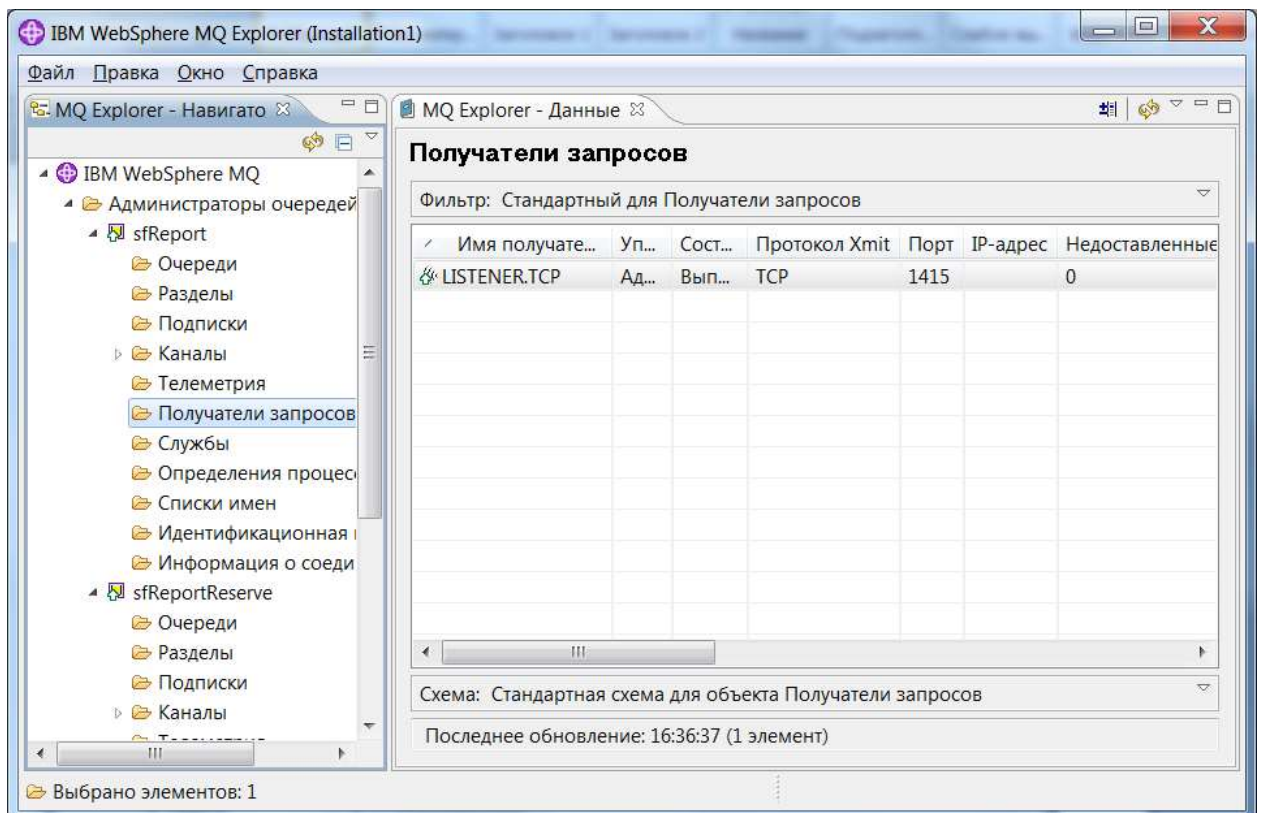


Рис. 53

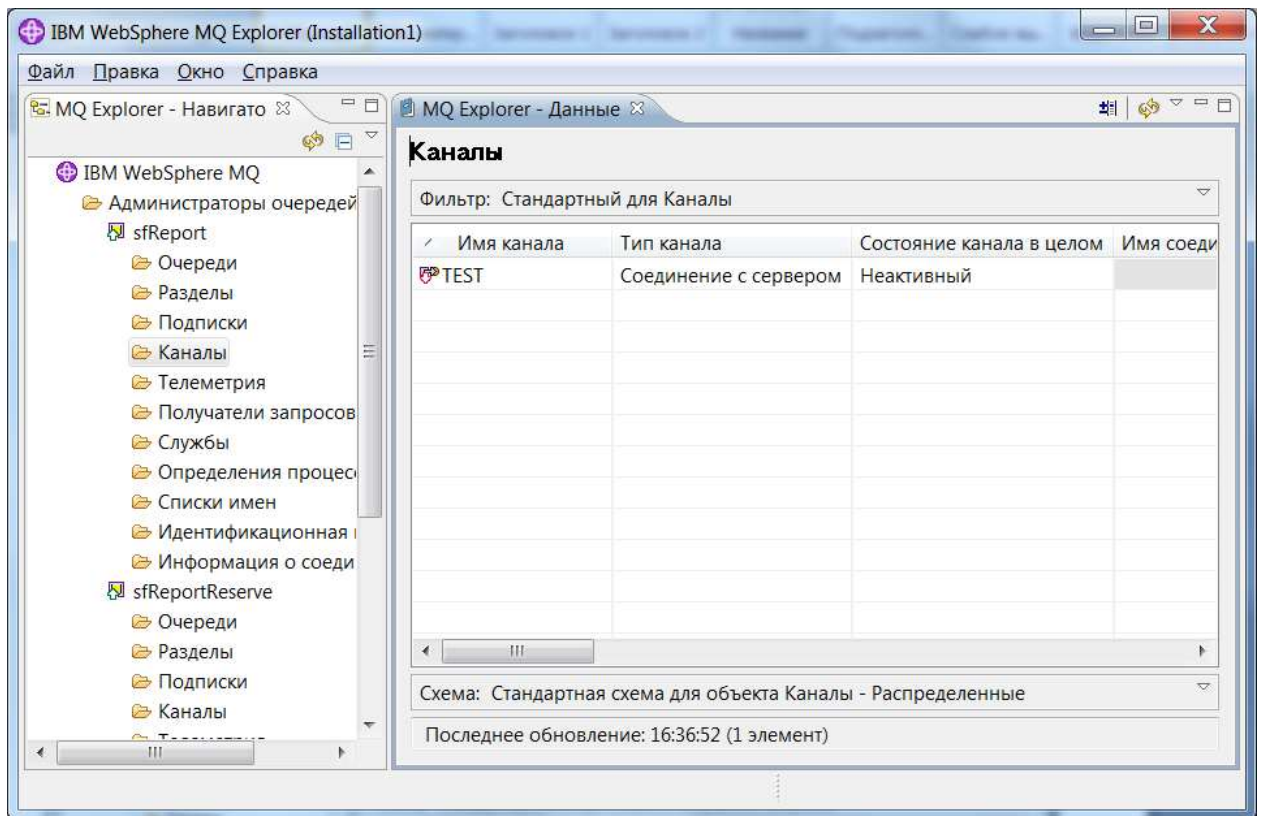


Рис. 54

17.2.2 MQ-авторизация

Дать права пользователю, под которым запущен CRE, на доступ к созданным менеджерам очередей и очередям. Например, одним из следующих способов:

- Использовать команду `setmqaut`. Пример:

```
setmqaut -m sfReport -t qmgr -p "login" +dsp +connect +inq
setmqaut -m sfReport -t queue -n queueIn -p "login" +passall +passid
+setall +setid +browse +get +inq +put +set
setmqaut -m sfReport -t queue -n queueOut -p "login" +passall +passid
+setall +setid +browse +get +inq +put +set
setmqaut -m sfReportReserve -t qmgr -p "login" +dsp +connect +inq
setmqaut -m sfReportReserve -t queue -n queueIn -p "login" +passall
+passid +setall +setid +browse +get +inq +put +set
setmqaut -m sfReportReserve -t queue -n queueOut -p "login" +passall
+passid +setall +setid +browse +get +inq +put +set
```

При этом предполагается, что CRE запущена под пользователем `"login"` и данный пользователь заведен на сервере MQ (если сервер MQ не в домене).

- Добавить пользователя в группу `mqm` (на сервере MQ) и обновить политику безопасности, выполнив MQSC-команду `REFRESH SECURITY(*)`

Примечание: для облегчения проведения тестирования можно отключить аутентификацию на канале при помощи MQSC-команды `ALTER QMGR CHLAUTH` и явно задать MCA User ID для канала соединения с сервером (например, указав в качестве MCA User ID группу `"mqm"`).

Команда для отключения аутентификации:

```
runmqsc sfReport
ALTER QMGR CHLAUTH(DISABLED)
```

```

END
runmqsc sfReserve
ALTER QMGR CHLAUTH(DISABLED)
END

```

Указание MCA User ID:

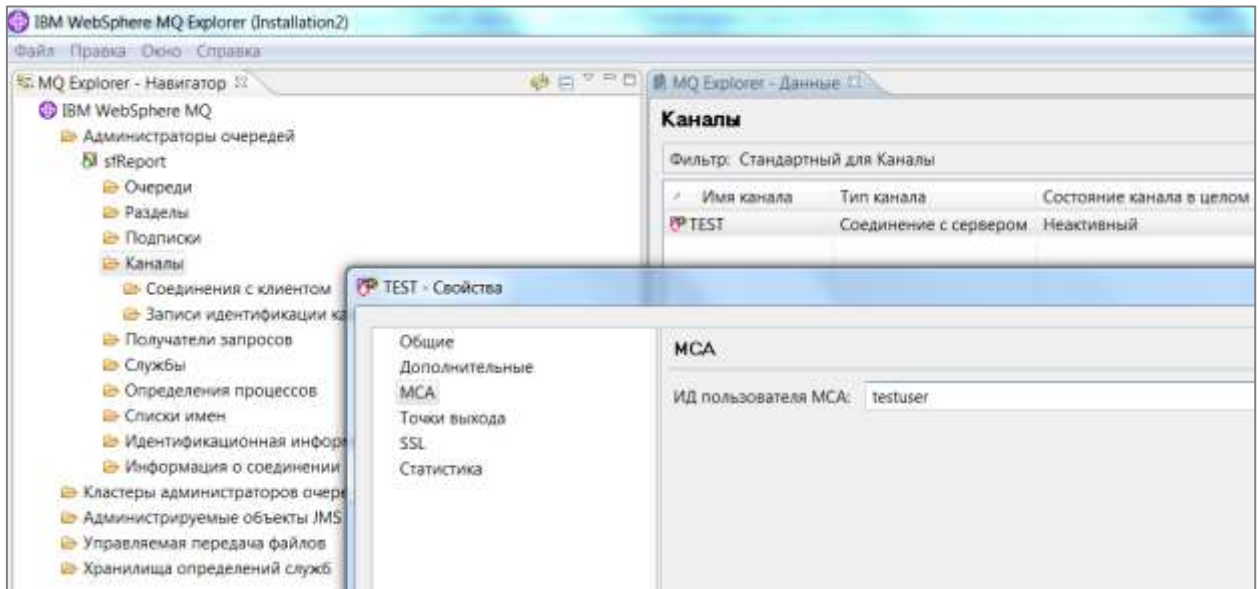


Рис. 55 Указание MCA User ID

После выполнения указанных команд рекомендуем перезапустить менеджер очередей.

17.3 Настройка сервера приложений (Tomcat)

1. Скопировать следующие файлы клиента MQ в каталог Tomcat/common/lib:

- com.ibm.mq.commonservices.jar
- com.ibm.mq.headers.jar
- com.ibm.mq.jar
- com.ibm.mq.soap.jar
- com.ibm.mqjms.jar
- connector.jar
- dhbcore.jar
- fscontext.jar
- jms.jar
- jndi.jar
- com.ibm.mq.jmqi.jar

2. Настроить JNDI-ресурсы, отредактировав файл Tomcat/conf/context.xml.

Пример строк, которые нужно добавить (желтым фоном выделены параметры, которые должны быть отредактированы согласно созданным очередям):

```

<Resource name="jms/WsQFactory"
  auth="Container"
  type="com.ibm.mq.jms.MQQueueConnectionFactory"
  factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"
  description="JMS Queue Connection Factory"
  HOST="127.0.0.1"
  PORT="1415"
  CHAN="TEST"

```

```

TRAN="1"
QMGR="sfReport"/>
<Resource name="jms/WsQueueIn"
auth="Container"
type="com.ibm.mq.jms.MQQueue"
factory="com.ibm.mq.jms.MQQueueFactory"
description="JMS Queue for recieve messages"
QU="queueIn"/>
<Resource name="jms/WsQueueOut"
auth="Container"
type="com.ibm.mq.jms.MQQueue"
factory="com.ibm.mq.jms.MQQueueFactory"
description="JMS Queue for send messages"
QU="queueOut"
TC="0"/>

<Resource name="jms/WsQFactoryReserve"
auth="Container"
type="com.ibm.mq.jms.MQQueueConnectionFactory"
factory="com.ibm.mq.jms.MQQueueConnectionFactoryFactory"
description="Reserve JMS Queue Connection Factory"
HOST="127.0.0.1"
PORT="1416"
CHAN="TEST"
TRAN="1"
QMGR="sfReportReserve"/>
<Resource name="jms/WsQueueInReserve"
auth="Container"
type="com.ibm.mq.jms.MQQueue"
factory="com.ibm.mq.jms.MQQueueFactory"
description="Reserve JMS Queue for recieve messages"
QU="queueIn"/>
<Resource name="jms/WsQueueOutReserve"
auth="Container"
type="com.ibm.mq.jms.MQQueue"
factory="com.ibm.mq.jms.MQQueueFactory"
description="Reserve JMS Queue for send messages"
QU="queueOut"
TC="0"/>

```

Имена ресурсов должны быть точно такими, как в приведенном примере (выделены **жирным**)!

Описание атрибутов ресурсов:

HOST	Имя/IP сервера, на котором размещен менеджер очередей
PORT	Порт
CHAN	Канал
TRAN	Тип транспорта: 0 – BINDINGS (Inter-Process Communication): данный вид транспорта рекомендуется использовать, если менеджер очередей располагается на той же машине, что и сервер приложений с CRE 1 – CLIENT (Remote Procedure Call): использовать сетевое соединение, рекомендуется для остальных случаев (когда невозможно использовать BINDINGS) 2 – DIRECT_TCPIP: real-time TCP/IP 4 – DIRECT_HTTP: real-time HTTP 8 – BINDINGS_THEN_CLIENT: сначала попытаться использовать BINDINGS. Если соединение не удастся, то использовать CLIENT. Для использования только в рамках JCA RA
QMGR	Менеджер очередей
QU	Очередь
TC	Тип целевого клиента:

- 0 – WMQ_CLIENT_JMS_COMPLIANT: получатель является JMS-приложением (заголовок RFH2 будет присутствовать) – значение по умолчанию
- 1 – WMQ_CLIENT_NONJMS_MQ: получатель является MQ-приложением (заголовок RFH2 не будет присутствовать)

17.4 Активация в CRE интерфейса взаимодействия через WebSphere MQ

Перейти в раздел *Администрирование* -> *Параметры* -> *Основные параметры* -> *Сервис IBM MQ*:

- установить галку «Активация запросов через IBM MQ»
- указать максимальное количество параллельных потоков через IBM MQ
- указать интервал подключений к MQ - (будет использоваться в случае возникновения ошибок, например, сетевых)
- если требуется получать сообщения в формате MQSTR (вместо MQRFH2), то установить соответствующую галку (при этом получатель должен быть MQ-приложением, TC="1")
- если требуется использовать JMSReplyTo, то установить соответствующую галку

Рис. 56 Параметры CRE для сервиса IBM MQ

18 Типичные ошибки при установке комплекса

1. При попытке зайти в программу Credit Registry из браузера или из Tomcat Manager возникает сообщение об ошибке “connection refused” (показано на рис. внизу). Ошибка говорит об отсутствии с базой MS SQL Server.

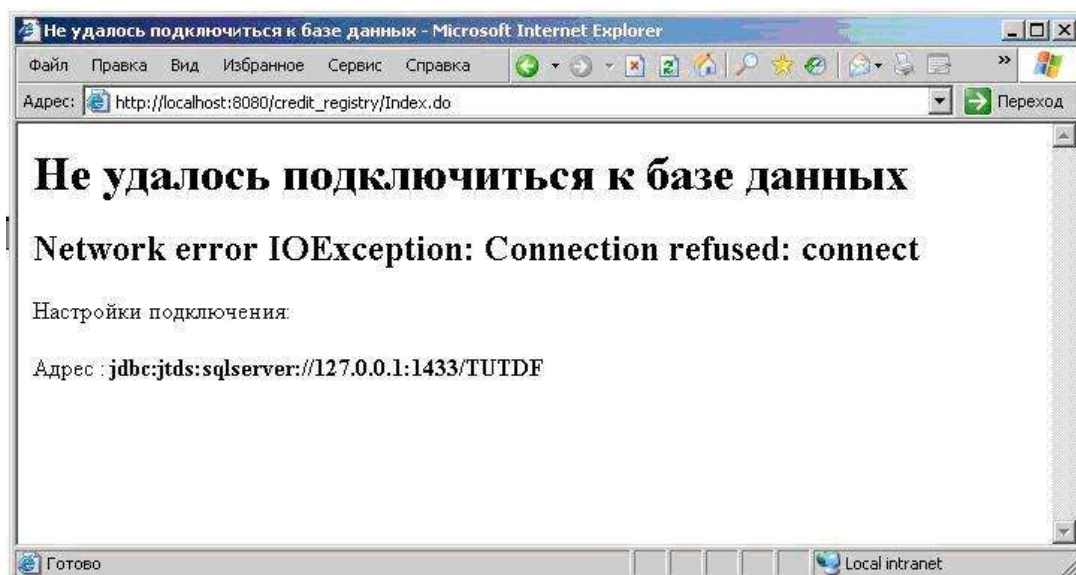


Рис. 57

Возможные причины возникновения ошибки:

- Не запущен SQL сервер. В файле Tomcat\conf\context.xml введены неверные параметры соединения с MS SQL Server, а именно: логин, пароль пользователя SQL сервера (по умолчанию: логин tutdf; пароль tutdf); IP-адрес, порт SQL сервера; название базы данных (по умолчанию используется база TUTDF);
- Программа типа firewall блокирует соединение.

Примечание: Необходимо помнить, что при изменении параметров в файле *hibernate.cfg.xml*, необходимо выполнить остановку и повторный запуск приложения *Credit_Registry* в списке приложений в *Tomcat Manager* (см. раздел 4 «Установка *Credit Registry*»), а при внесении изменений в *server.xml* – перезапустить сервис *Tomcat*.

19 Мониторинг работы коннекторов

19.1 Доступ к данным мониторинга

Для входа на страницу мониторинга введите в адресной строке браузера адрес системы Credit Registry, в качестве примера приведем ссылку на демонстрационный сервер МТЦ: http://demo.creditregistry.ru:8080/credit_registry/, после чего добавьте к адресу следующую строку: "statusMonitor".

Таким образом, адрес страницы мониторинга в приведенном примере будет выглядеть следующим образом: http://demo.creditregistry.ru:8080/credit_registry/statusMonitor

Аутентификация и авторизация не требуется.

В ответ система возвращает plain text страничку в кодировке windows-1251.

Пример странички приведен ниже:

```
Overall (count,min,avg,max) :❶
NBCH Emulator.bureau_time: 28883, 0, 62, 610
NBCH Emulator.queue_time: 29042, 0, 0, 250
NBCH Emulator.service_time: 28883, 31, 203, 29839
NBCH Emulator.request_time: 28883, 0, 64, 625
NBCH Emulator.errors: 159, 1, 1, 1
NBCH Emulator.requests: 29042, 1, 1, 1
NBCH Emulator.net_errors: 159, 1, 1, 1

Current (count,min,avg,max) :❷
NBCH Emulator.bureau_time: 382, 0, 71, 515
NBCH Emulator.queue_time: 382, 0, 0, 16
NBCH Emulator.service_time: 382, 32, 205, 1406
NBCH Emulator.request_time: 382, 0, 73, 515
NBCH Emulator.errors: 0, 0, 0, 0
NBCH Emulator.requests: 382, 1, 1, 1
NBCH Emulator.net_errors: 0, 0, 0, 0

❶ Overall секция статистики
❷ Current секция статистики
```

Рис. 58 – Данные мониторинга

19.2 Overall и Current разделы статистики

Вся статистика делится на два раздела: Overall и Current

- Overall – статистика собирается и ведется с момента запуска системы;
- Current – статистика собирается и ведется за последние 5 минут работы системы, события учитываются с задержкой в 10 секунд.

19.3 Правила именования и значения параметров

Параметры именуются по следующему шаблону

<Имя_Профиля_Коннектора>.<Имя_Параметра>

Для каждого параметра перечисляются следующие значения:

- count – количество событий за измеряемый период;
- min – минимальное значение для события за измеряемый период;
- avg – среднее значение для события за измеряемый период;
- max – максимальное значение для события за измеряемый период.

Для параметров с суффиксом *_time* значение события – время в миллисекундах.

Для параметров "счётчиков" значение события всегда 1 (сам факт наступления события).

Если событие не происходило в измеряемом периоде, то статистика по нему может не выводиться, в этом случае можно считать, что значение его параметров равно 0, 0, 0, 0.

19.4 Измеряемые параметры и события

В системе ведётся учёт и измерение следующих событий:

Параметр	Описание события
<i>requests</i>	Общее количество запросов поступивших на коннектор
<i>errors</i>	Общее количество ошибок всех типов, включает в себя детализируемые ниже ошибки
<i>timeout_errors</i>	Количество ошибок по причине тайм аутов ответа БКИ или внешнего источника
<i>gate_conn_errors</i>	Количество ошибок по причине ошибок соединений с SSLGate
<i>gate_conn_time</i>	Количество и общие продолжительности успешных соединений через SSLGate, позволяет оценить эффективность удержания и использования одного SSL соединения для выполнения нескольких запросов
<i>bki_conn_errors</i>	Количество ошибок по причине ошибок/таймаутов соединений с БКИ
<i>net_errors</i>	Количество других сетевых ошибок (SSLGate<->БКИ)
<i>bki_status_errors</i>	Количество ошибок БКИ или внешнего источника в прикладном протоколе. Например, для НБКИ - статус HTTP ответа не 200
<i>queue_timeouts</i>	Количество ошибок по причине тайм аутов ожидания в очереди коннектора
<i>request_time</i>	Количество и общие продолжительности непосредственных обращений в БКИ или внешний источник по успешным запросам (не учитываются запросы окончившиеся ошибками)

<i>service_time</i>	Количество и общие продолжительности по успешным запросам с учётом всех накладных расходов - авторизации, чтения записи БД и т.д. То есть (service_time - request_time) это время суммарных накладных расходов Credit Registry при выполнении запроса и регистрации-анализа ответа
<i>bureau_time</i>	Количество и продолжительности ожидания ответа БКИ или внешнего источника по успешным запросам (не учитываются запросы окончившиеся ошибками)
<i>queue_time</i>	Количество и продолжительности ожидания в очереди успешно запросов, не превысивших ограничение по времени ожидания в очереди для данного профиля коннектора
<i>login_wait_time</i>	Время ожидания свободного логина для выполнения запроса в ОКБ (в CRE может выстраиваться очередь, т.к. ОКБ на своей стороне запросы от одного логина обрабатывает последовательно)
<i>SSLGate_sign_errors</i>	Количество ошибок формирования ЭЦП для запросов (SSLGate)
<i>SSLGate_sign_time</i>	Количество и продолжительности формирования успешных ЭЦП для запросов (SSLGate)
<i>SSLGate_sign_timeouts</i>	Количество таймаутов при формировании ЭЦП для запросов (SSLGate)
<i>request_parallel_count</i>	Количество запросов исполняемых параллельно на конкретном типе коннектора
<i>bureau_request_parallel_count</i>	Количество запросов исполняемых параллельно в бюро на конкретном типе коннектора
<i>errors_wo_retries</i>	Количество цепочек запросов, завершившихся технической ошибкой
<i>bureau_error_status_wo_retries</i>	Количество цепочек запросов, завершившихся приемом от бюро корректного сообщения с информацией об ошибке (BUREAU_STATUS=2 в таблице CONNECTOR_DATA)
<i>requests_wo_retries</i>	Количество цепочек запросов (общее)

20 Настройка курсов валют

Курсы валют в Credit Registry используются для отчетов единого формата (модуль УСО).

Используются для пересчета на рубли сумм, указанных в валюте, отличной от рубля.

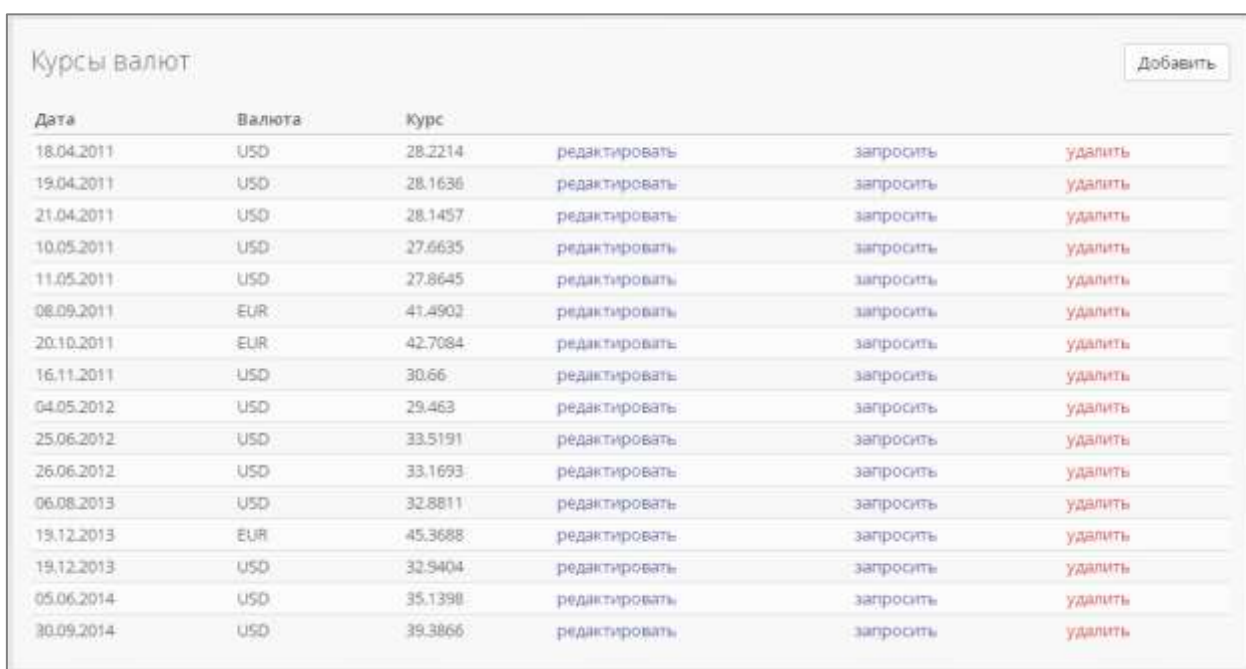
Курс валюты может быть взят из локальной БД, либо может быть запрошен с сайта ЦБ.

Для запроса курса валют с сайта ЦБ должен быть открыт доступ с сервера CreditRegistry на сайт www.cbr.ru по порту 80.

Определение курса валюты происходит следующим образом:

1. Курс хранится в БД. При старте CRE загружает таблицу курсов из БД.
2. При расчёте нагрузки клиента CRE использует загруженный курс.
3. Если курс на заданную дату не определён, CRE запрашивает его через публичный веб-сервис ЦБ РФ. Полученный курс применяется для расчёта и вносится в БД для дальнейшего использования.
4. Если веб-сервис недоступен и на заданную дату курс не найден, CRE использует ближайший по дате курс этой валюты (поиск назад).
5. Если исторические данные так же не найдены, CRE использует курс из БД, дату 1 января 1900 года (курс по умолчанию).
6. Если и такой курс не найден, конвертация не производится (берётся курс = 1).

В интерфейсе можно указать для каждой валюты курс по отношению к рублю – курс за конкретную дату, либо курс по умолчанию (т.е. на дату 01.01.1900).



Дата	Валюта	Курс			
18.04.2011	USD	28.2214	редактировать	запросить	удалить
19.04.2011	USD	28.1636	редактировать	запросить	удалить
21.04.2011	USD	28.1457	редактировать	запросить	удалить
10.05.2011	USD	27.6635	редактировать	запросить	удалить
11.05.2011	USD	27.8645	редактировать	запросить	удалить
08.09.2011	EUR	41.4902	редактировать	запросить	удалить
20.10.2011	EUR	42.7084	редактировать	запросить	удалить
16.11.2011	USD	30.66	редактировать	запросить	удалить
04.05.2012	USD	29.463	редактировать	запросить	удалить
25.06.2012	USD	33.5191	редактировать	запросить	удалить
26.06.2012	USD	33.1693	редактировать	запросить	удалить
06.08.2013	USD	32.8811	редактировать	запросить	удалить
19.12.2013	EUR	45.3688	редактировать	запросить	удалить
19.12.2013	USD	32.9404	редактировать	запросить	удалить
05.06.2014	USD	35.1398	редактировать	запросить	удалить
30.09.2014	USD	39.3866	редактировать	запросить	удалить

Рис. 59 Курсы валют

Для редактирования курсов валют в роли пользователя должна быть поставлена опция – «задание значений курсов валют».

Основные параметры

Название роли:

Описание роли:

Приоритет роли: (0-1000)

- Редактирование пользователей и прав
- Редактирование дополнительных параметров
- Редактирование группы
- Редактирование справочника кредитных программ
- Редактирование кода участника НБКИ
- Редактирование РНКО (ЦБ ЦККИ)
- Редактирование справочника ТУ и филиалов
- Редактирование справочника сертификатов
- Редактирование списков рассылок
- Редактирование стратегий триггеров
- Групповые запросы
- Пакетные запросы
- Сведение пакетных ответов
- Поточковые запросы
- Сохранение отчетов в Базу Данных
- Очистка кредитных историй субъектов от старых изменений
- Загрузка данных пакетного отчета КИ
- Настройка логирования системы
- Изменение данных в истории запросов
- Задание значений курсов валют**
- Статус фоновых задач

Рис. 60 Право «Задание значений курсов валют»

Рекомендации по настройке:

Для корректной работы конвертации курсов валют рекомендуется использовать один из способов:

- Получать данные из локальной базы данных или при помощи соединения с публичным веб-сервисом ЦБ РФ;
- Использовать флаг в настройках CRE: Настройки единого формата -> Отключить конвертацию валют в рубли.

ПРИЛОЖЕНИЕ А. Инструкция по установке ключей CryptoPro для SSLGate

Предполагается, что КриптоПро CSP уже установлен.

Примечание: после установки КриптоПро CSP необходимо перезагрузить компьютер для завершения установки КриптоПро CSP.

Для установки сертификатов необходима дискета с закрытым ключом (или ее образ), сертификат к закрытому ключу и сертификат удостоверяющего центра. Закрытый ключ будет устанавливаться в реестр.

Примечание. Сертификат можно устанавливать с привязкой закрытого ключа как из реестра, так и с дискеты и токена, тем не менее, настоятельно рекомендуется копировать ключ в реестр и устанавливать сертификат с привязкой закрытого ключа именно из реестра. Это предотвратит проблемы с возможными «подвисаниями» токена и износом дискеты.

Для того чтобы установить личный сертификат в личные сертификаты локального компьютера с хранением закрытой части ключа в реестре, нужно выполнить следующие действия:

1. Копирование ключей в реестр в хранилище локального компьютера
2. Установка личного сертификата (привязка открытой части ключа к контейнеру с закрытой частью ключа)
3. Установка сертификатов удостоверяющего центра.

1. Копирование ключей в реестр

Ключи должны быть на дискете, или можно использовать виртуальную дискету, созданную программой типа ImDisk Virtual Disk Driver (<http://www.ltr-data.se/opencode.html/>).

1. Установите ключевую дискету в дисковод, или запустите виртуальную дискету.
2. Запустите КриптоПро CSP из панели управления. CryptoPro может не увидеть виртуальную дискету, если панель была открыта во время подключения дискеты. На вкладке «Общие» нажмите на гиперссылку «Запустить с правами администратора»
3. На закладке «Сервис» нажмите кнопку «Скопировать...».
4. Нажмите кнопку «Обзор...», выберите необходимый контейнер, нажмите кнопку «ОК» и нажмите кнопку «Далее».
5. Введите имя для нового контейнера, в разделе «Введенное имя задает ключевой контейнер» выберите «Компьютера» и нажмите кнопку «Готово»
6. В появившемся окне в разделе «Устройства» выберите «Реестр» и нажмите кнопку «ОК»
7. В появившемся окне нажмите кнопку «ОК» (пароль на контейнер задавать не надо).

2. Установка личного сертификата (привязка открытой части ключа к контейнеру с закрытой частью ключа)

1. Запустите КриптоПро CSP из панели управления. На вкладке «Общие» нажмите на гиперссылку «Запустить с правами администратора»
2. На закладке «Сервис» нажмите кнопку «Установить личный сертификат...».
3. Нажмите кнопку «Обзор», выберите нужный сертификат и нажмите кнопку «Далее».
4. В окне «Сертификат для установки» проверьте что выбран корректный сертификат и нажмите кнопку «Далее»

5. В разделе «Введенное имя задает ключевой контейнер» выберите «Компьютера», в поле «Имя ключевого контейнера» нажмите кнопку «Обзор», выберите ключевой контейнер, который Вы задавали в п.5 при копировании ключа в реестр и нажмите кнопку «Далее»
6. В окне «Хранилище сертификатов» убедитесь, что в поле «Имя хранилища сертификатов» выбрано «Личное» и в разделе «Используются хранилища сертификатов» выбрано «Компьютера», нажмите кнопку «Далее»
7. В окне «Завершение работы мастера установки личного сертификата» нажмите на кнопку «Готово».

3. Установка сертификатов удостоверяющего центра

1. Запустите Microsoft Management Console: в меню «Пуск» - «Выполнить» - введите mmc и нажмите кнопку «ОК».
2. В меню «Файл» выберите «Добавить или удалить оснастку...».
3. Выберите из списка пункт «Сертификаты» и нажмите кнопку «Добавить».
4. В окне «Оснастка диспетчера сертификатов» выберите «Учетной записи компьютера» и нажмите кнопку «Далее».
5. В окне «Выбор компьютера» выберите «Локальным компьютером» и нажмите кнопку «Готово».
6. В окне «Добавление и удаление оснасток» Нажмите кнопку «ОК».
7. В дереве папок выберите «Доверенные корневые центры сертификации» нажмите правой кнопкой мышки на этой папке и в контекстном меню выберите «Все задачи – Импорт...».
8. В окне «Мастер импорта сертификатов» нажмите кнопку «Далее».
9. Нажмите кнопку «Обзор», выберите файл с сертификатом/сертификатами и нажмите кнопку «Далее».
10. Убедитесь, что в появившемся окне выбрано «Поместить все сертификаты в следующее хранилище – Доверенные корневые центры сертификации» и нажмите кнопку «Далее».
11. В окне «Завершение мастера импорта сертификатов» нажмите кнопку «Готово».

4. Проверка правильности установки личного сертификата

Для корректной установки сертификата достаточно предыдущих трех пунктов данного приложения. Если сертификат установлен некорректно, после установки сертификата при запросе в БКИ будут какие-либо ошибки подписи. Если быстро понять причину ошибки не удастся, рекомендуется обратиться в нашу техподдержку.

Список основных проверок:

1. В консоли mmc в закладке «Сертификаты (локальный компьютер)» проверить, что только что установленный сертификат есть в папке «Личное - Сертификаты».
2. Открыть установленный сертификат двойным щелчком, проверить, что на вкладке «Общие» внизу есть надпись: «Есть закрытый ключ для этого сертификата», во вкладке «Путь сертификации» корректно сформирован путь до корневого сертификата и сертификаты установлены без ошибок.

3. В ММС-консоли, в закладке «Сертификаты (локальный компьютер)»-«Доверенные корневые центры сертификации» должны быть все актуальные сертификаты УЦ КРИПТО-ПРО.
4. (Для тестовых сертификатов и сертификатов для запросов в БРС и Equifax). В свойствах сертификата на закладке «Путь сертификации» проверить, какой сертификат указан корневым. Если это не УЦ КРИПТО-ПРО (в частности, если это тестовый центр КриптоПро или другой УЦ), этот сертификат тоже должен отображаться в консоли в закладке «Доверенные корневые центры сертификации».

Примечание: если корневым сертификатом указан не УЦ КРИПТО-ПРО, корневые сертификаты УЦ КРИПТО-ПРО все равно должны быть установлены.

5. После установки сертификатов был перезапущен SSLGate.
6. На контейнер закрытого ключа пароль должен либо не ставиться, либо при установке личного сертификата при вводе пароля необходимо поставить галочку – «сохранить пароль». Если Вы не уверены, выполнено ли это условие, необходимо повторить установку личного сертификата (см. раздел 3 данного приложения.)

Внимание! Если пароль на контейнер есть, но при создании контейнера не была поставлена галочка "сохранить пароль", при установке сертификата пароль может не спрашиваться, но при запросе в БКИ пароль потребуется и SSLGate не сможет его "ввести". Рекомендуется для проверки этого пункта дополнительно скопировать закрытый ключ в новый контейнер без пароля и повторить установку сертификата с привязкой к новому контейнеру.

7. Если закрытый ключ не скопирован в реестр (это не рекомендуемый вариант), то хранилище ключей (дискета, токен, виртуальная дискета, флэш-диск) должно быть вставлено в компьютер и должно отображаться в списке доступных считывателей в «Панель управления -> КриптоПро CSP -> вкладка «Оборудование» -> кнопка «Настроить считыватели...»»
8. Если закрытый ключ скопирован в реестр, то при установке личного сертификата (раздел 3 данного приложения) должен быть указан контейнер именно из реестра и именно из хранилища компьютера, а не пользователя.
9. В свойствах сервиса SSLGate на закладке logon рекомендуем выставить галочку «разрешить взаимодействие с рабочим столом».

ПРИЛОЖЕНИЕ В. Рекомендации по установке нескольких копий приложения

Настоятельно рекомендуется не устанавливать на один Tomcat несколько копий приложения Credit Registry. Если необходимо установить несколько экземпляров Credit Registry на одном сервере, следует также установить несколько экземпляров Tomcat.

Сделать это можно следующим образом:

1. Скачать Tomcat (но не сервис-installer) по ссылке <http://tomcat.apache.org/download-70.cgi>
2. Распаковать архив «32-bit Windows.zip» или «64-bit Windows.zip». Запустить командный файл «/bin/service.bat» через файловый менеджер (например, far) с параметрами:
 - *install [имя сервиса]*
например,
service.bat install CRE
 - Имя сервиса необходимо указывать без пробелов.
3. Изменить название файла «/bin/tomcat7w.exe» на «/bin/CREw.exe».
4. В конфигурации «conf/server.xml» для разных экземпляров Tomcat должны быть указаны различные порты

connectorport (по умолчанию 8080) и

serverport (по умолчанию 8005)

например, Connectorport="8080", Serverport = "8005" для одного экземпляра Tomcat, Connectorport="8081", Serverport = "8006" для другого.

5. Убедиться, что в «conf/tomcat-users.xml» пользователю «admin» присвоена роль «manager-gui»:

```
<user username="admin" password="admin" roles="admin-gui,manager-gui" />
```

6. Зайти в сервисы, запустить новый сервис – Apache Tomcat CRE.

ПРИЛОЖЕНИЕ С. Установка новых версий приложения

Предполагается, что Tomcat установлен в директорию C:\Program Files\Apache Software Foundation\Tomcat 7.0\

Чтобы установить новую версию CreditRegistry необходимо сделать следующее:

1. остановите службу Tomcat;
2. сделайте резервное копирование базы данных CreditRegistry (резервное копирование делается стандартными средствами MSSQL/Oracle/PostgreSQL) и файла \webapps\credit_registry.war
3. в директории \webapps удалите файл credit_registry.war и директорию credit_registry;
4. удалите содержимое директории \temp (саму папку \temp удалять не надо);
5. удалите содержимое директории \work (саму папку \work удалять не надо);
6. скопируйте файл credit_registry.war (новой версии CreditRegistry) в директорию \webapps;
7. запустите Tomcat.

Если обновление прошло успешно, то файлы, полученные в п.2 можно удалить, если при обновлении системы произошли ошибки, то для отката изменений необходимо сделать следующее:

1. остановите службу Tomcat;
2. в директории \webapps удалите файл credit_registry.war и директорию credit_registry;
3. удалите содержимое директории \temp (саму папку \temp удалять не надо);
4. удалите содержимое директории \work (саму папку \work удалять не надо);
5. восстановите из резервной копии базу данных, соответствующую предыдущей версии CreditRegistry и скопируйте файл credit_registry.war от предыдущей версии в папку \webapps
6. запустите Tomcat.

Примечание: При использовании SQL Server в качестве СУБД при обновлении CreditRegistry с версии младше 7.15 до версии 7.15 или выше необходимо использовать соответствующие драйвера подключения к серверу баз данных и внести необходимые изменения в файл context.xml (подробнее см. в п. «[5.2 Конфигурация соединения с базой данных](#)»). Также необходимо обратить внимание на используемую версию SQL Server (для CreditRegistry младше 7.15 допустимо использование MSDE или SQL Server 2000-2005)

ПРИЛОЖЕНИЕ D. Настройка SSLGate для работы с ЦККИ

Требуемое ПО и ключи

1. СКЗИ Верба-OW. Дистрибутив и лицензия на это ПО должны быть в банке. В частности, они должны быть у отдела, занимающегося отправкой банковской отчетности в ЦБ.
Примечание: Верба для 64 битных ОС не сертифицирована.
Верба для 32 битных ОС сертифицирована.
2. Дискета с «Вербовскими» ключами. Эти ключи используются, в частности, для подписания и шифрования банковской отчетности для отправки в ЦБ.
3. Утилита SCSignEx. Используется для подписания и шифрования файлов «вербовскими» ключами. Разработчиком данной утилиты является ЦБ. Дистрибутив данной утилиты должен быть в банке, либо может быть запрошен у ЦБ. **Примечание.** При тестировании была использована версия 4.1.2.3. Рекомендуется использовать версии не ниже 4.*.
4. Архиватор ARJ32. Дистрибутив есть на сайте www.arjsoftware.com. В частности, можно использовать версию ARJ32 3.20. Также дистрибутив arj можно скачать здесь: http://arj.sourceforge.net/files/arjw_310.exe
5. Версия SSLGate должна быть не ниже 4.10
Примечание: для работы SSLGate версии 3.0 и выше необходим NET Framework 3.5.

Шаги установки

Настройка «СКЗИ Верба-OW»

1. Установить СКЗИ Верба-OW на компьютер с SSLGate. Дистрибутив и лицензия на это ПО должны быть в банке. В частности, они должны быть у отдела, занимающегося отправкой банковской отчетности в ЦБ.
2. Вставить дискету или подключить виртуальную дискету с ключами. В качестве ключевого носителя может также выступать флэш-накопитель. Локальный диск как ключевой носитель использоваться не может (т.к. Верба просто «не увидит» ключи, хранящиеся просто на диске).
3. Запустить «модуль загрузки ключей». Пуск, все программы, Верба-OW, модуль загрузки ключей.
4. Двигая мышью, проинициализировать генератор случайных чисел.
Внимание! Инициализацию генератора случайных чисел необходимо выполнять под тем пользователем, под которым будет запущен SSLGate. Если инициализация генератора случайных чисел уже была произведена под другим пользователем, необходимо перезагрузить компьютер и повторить инициализацию.
5. В интерфейсе «Модуля загрузки ключей» выбрать дискету с ключами. Для проверки успешности настройки нажать «загрузить», а затем «выгрузить». Примечание. В конце проверки список загруженных ключей должен быть пуст.
6. Выйти из «Модуля загрузки ключей».

Установка архиватора ARJ

7. Установить ARJ32 на компьютере с SSLGate. Дистрибутив есть на сайте www.arjsoftware.com, а также может быть получен у ЦБ. В частности, можно использовать версию ARJ32 3.15.

Настройка утилиты SCSignEx для работы со "СКЗИ Верба-OW"

8. Установить SCSignEx на компьютере с SSLGate. Дистрибутив можно получить либо в ЦБ, либо в отделе вашего банка, занимающемся отправкой отчетности в ЦБ.

9. Запустить и настроить SCSignEx. (Пуск, все программы, SignatureSC, SCSignEx)

Пример стандартных настроек:

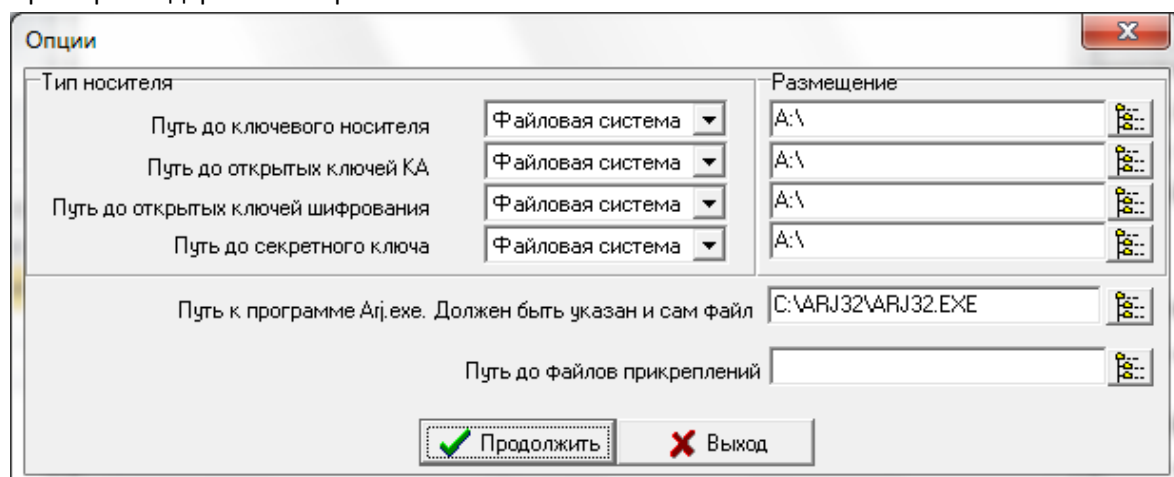


Рис. 61

В качестве «Размещения» везде указывается путь к дискете с ключами.

Путь к программе Arj.exe – путь к файлу Arj.exe архиватора ARJ.

10. Проверить, что SCSignEx настроен корректно: в интерфейсе SCSignEx выбрать произвольный файл для шифрования (кнопка open в SCSignEx), и нажать «установить КА и зашифровать на МГТУ». Если это действие выполнится без ошибок, SCSignEx настроен верно.

11. Проверить, что имя пользователя, под которым будет запускаться SSLGate и модуль загрузки ключей, не содержит знаков "-". Если имя пользователя содержит тире, необходимо в свойствах компьютера, на вкладке "дополнительно", в переменных среды указать значение переменных TMP и TEMP, не содержащее знак тире. Например, C:\Temp\

Примечание. Эта папка должна быть существующей.

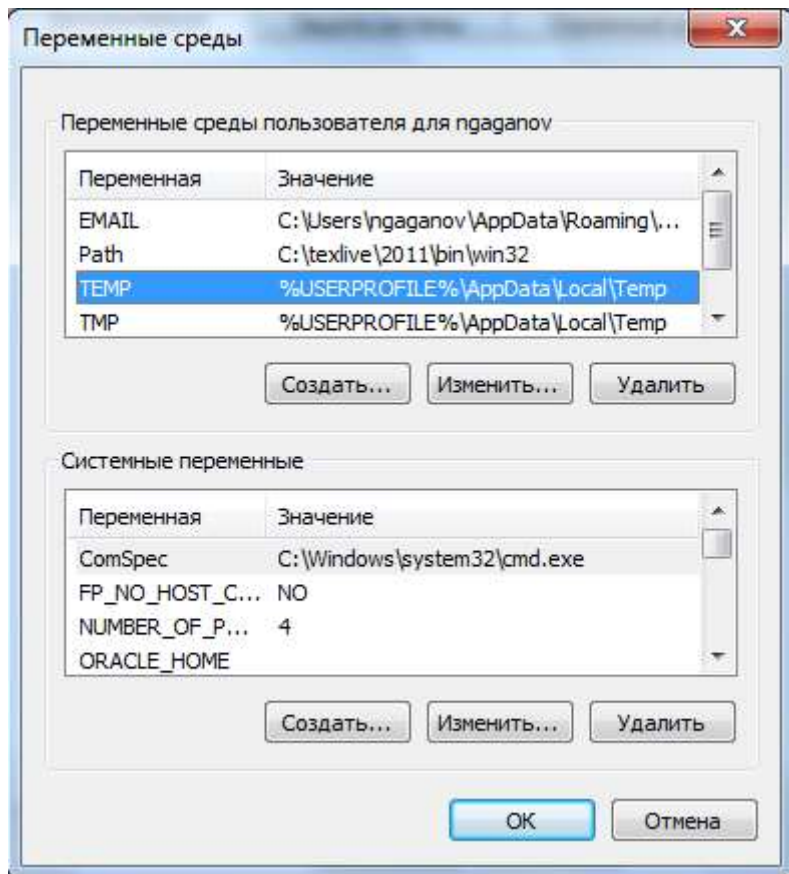


Рис. 62

Настройка SSLGate

12.
 - a. Если SSLGate не установлен, запустить установщик (SSLGate***setup.exe)
 - b. Если SSLGate уже установлен, необходимо забэкапить SSLGate.ini, удалить папку C:\Program Files\SSLGate, запустить установщик SSLGate, и после установки заменить SSLGate.ini на забэкапленный.
13. Добавить в SSLGate.ini раздел, отвечающий за взаимодействие с ЦБЦККИ.

```
[СККИ]
arj=C:\ARJ32\ARJ32.EXE
scsignex=C:\Program Files\MGTU Bank of Russia\SignatureSC\SCSignEx.exe
cmd_timeout=60000
```

Проверить, что указаны актуальные пути.

arj – путь к запускаемому файлу архиватораARJ

scsignex – путь к утилите SCSignEx

cmd_timeout – таймаут выполнения одиночных команд (в миллисекундах)

14. В панели управления операционной системы, в разделе администрирования необходимо запустить надстройку «Службы» (“Services”), найти службу “CreditRegistry SSLGate”.
15. В свойствах службы на закладке «Вход в систему» (“Log On”) указать пользователя и пароль, под которыми был проинициализирован Верба-OW:

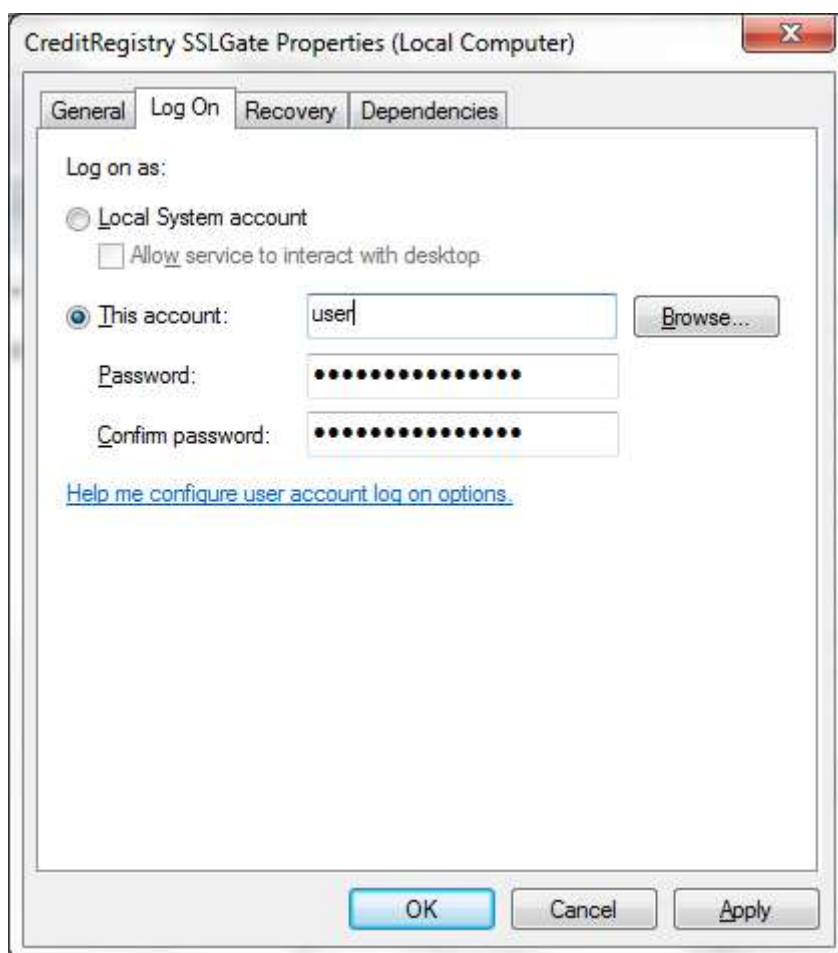


Рис. 63

16. На закладке «Общие» (“General”) значение «Тип запуска» (“Startup type”) должно быть «Вручную» (“Manual”).

Примечание. При автоматическом запуске SSLGate выявлены проблемы с инициализацией модуля загрузки ключей в Вербе, поэтому на данный момент мы не рекомендуем автоматический запуск SSLGate. Стоит отметить, что дополнительные действия при перезапуске сервера с SSLGate все равно потребуются – в частности, инициализация модуля загрузки ключей для Вербы, которую невозможно автоматизировать.

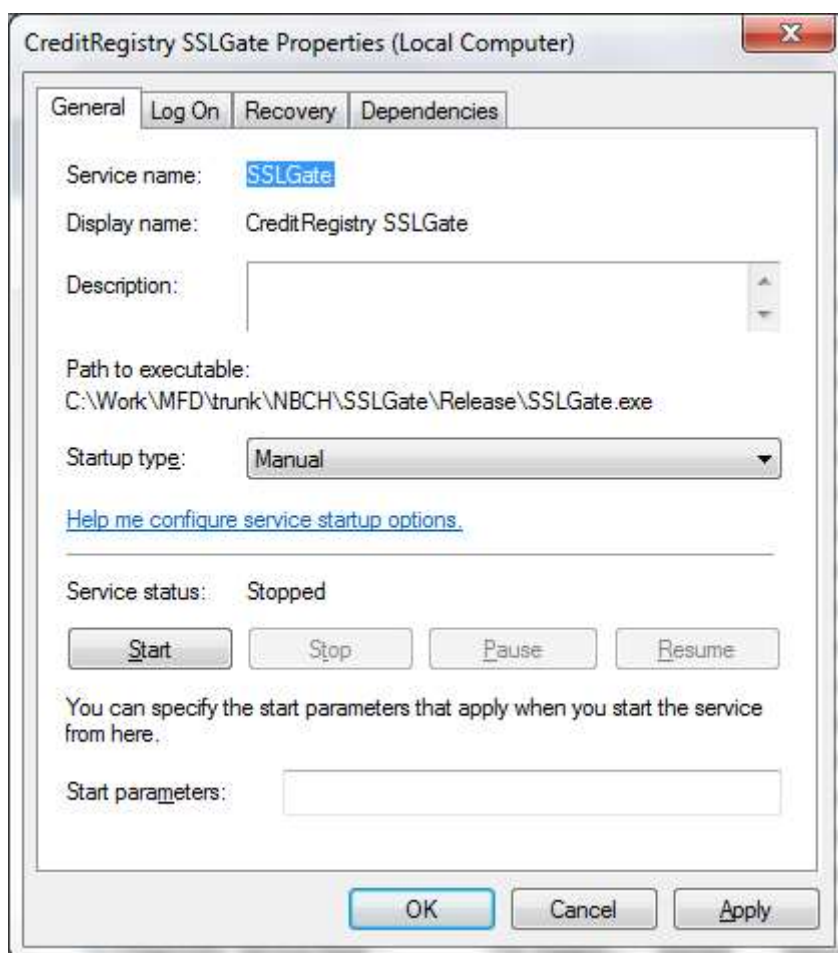


Рис. 64

17.3. Запустить SSLGate.

Действия после перезапуска сервера с SSLGate

После каждого перезапуска компьютера с SSLGate необходимо делать следующее:

1. Провести инициализацию модуля загрузки ключей Верба-OW: Пуск, все программы, Верба-OW, модуль загрузки ключей.
2. Двигая мышью, проинициализировать генератор случайных чисел.
3. В интерфейсе «Модуля загрузки ключей» выбрать дискету с ключами. Для проверки успешности настройки нажать «загрузить», а затем «выгрузить». Примечание. В конце проверки список загруженных ключей должен быть пуст.
4. зайти в панель управления операционной системы, в раздел администрирования, запустить надстройку «Службы» (“Services”), найти службу “CreditRegistry SSLGate” и запустить ее с помощью кнопки «Запустить» (“Start”).
5. Можно выйти из системы (Logoff), служба “CreditRegistry SSLGate” дальше будет работать в автономном режиме.

ПРИЛОЖЕНИЕ Е. Установка новых версий SSLGate

Возможно 2 варианта установки новой версии SSLGate:

- 1) Из установщика (из «SSLGate***setup.exe»):

В данном случае необходимо бэкапить файл sslgate.ini;

- 2) Заменой exe-файла установщика:

При варианте замены установщика необходимо новому exe-файлу присвоить то же имя, что было у прежнего exe-файла. Например: если новый exe-файл называется «SSLGateNet.exe», а прежний назывался «sslgate.exe», то новый нужно переименовать в «sslgate.exe».

ПРИЛОЖЕНИЕ F. Настройки, связанные с изменением временных зон

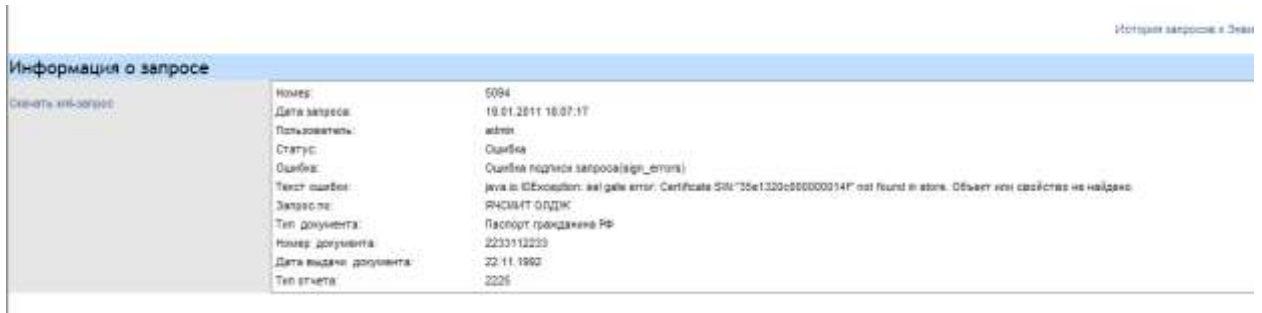
Если в интерфейсе Credit Registry отображается некорректное время, необходимо проверить следующее:

1. Какой часовой пояс указан в настройках Windows. Должен быть указан: «(UTC+03:00) Москва, Санкт-Петербург, Волгоград». Если указан другой часовой пояс, необходимо установить соответствующее обновление:
<https://support.microsoft.com/en-us/kb/3162835>
2. Если время в ОС отличается от времени в интерфейсе Credit Registry (или, что то же самое, время в ОС отличается от времени в логах stdout) на 1 час, необходимо установить актуальную версию java: <https://www.java.com> после чего изменить настройки Tomcat на использование актуальной версии Java и перезапустить службу Tomcat.
Так же, можно воспользоваться утилитой Java Time Zone Updater Tool:
<http://www.oracle.com/technetwork/java/javase/tzupdater-readme-136440.html>
Файл tzupdater.jar от актуальной версии Java необходимо скопировать в папку java\bin и выполнить команду:
`java.exe -jar tzupdater.jar -l`
После этого необходимо перезапустить Tomcat
Соответствие между Timezone Tzdata Version и версией JRE можно посмотреть на странице:
<http://www.oracle.com/technetwork/java/javase/tzdata-versions-138805.html>
3. Если используется БД Oracle, соединение с БД настроено через context.xml и будет использоваться автоматический импорт, необходимо заменить драйвер для соединения с Oracle в tomcat7\lib. Актуальный драйвер (ojdbc7.jar) можно скачать по странице:
<http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html>
4. Если время в ОС отличается от времени в интерфейсе Credit Registry (или время в ОС отличается от времени в логах stdout) и выполнены рекомендации 1-3, необходимо в настройках Tomcat'a (пуск – Apache Tomcat – Configure Tomcat) на вкладке Java добавить опцию:
`-Duser.timezone=Europe/Moscow`
После этого необходимо перезапустить Tomcat.

ПРИЛОЖЕНИЕ G. Типичные ошибки настройки коннекторов

Ошибка подписи запроса (sign_errors)

java.io.IOException: ssl gate error: Certificate S\N:"519a549900020000654c" not found in store. Объект или свойство не найдено



Информация о запросе	
Скачать xml-запрос	Номер: 5094
	Дата запроса: 19.01.2011 10:07:17
	Пользователь: admin
	Статус: Ошибка
	Ошибка: Ошибка подписи запроса(sign_errors)
	Текст ошибки: java.io.IOException: ssl gate error: Certificate S\N:"519a549900020000654c" not found in store. Объект или свойство не найдено
	Запрос по: ЯСМИНТ ОЛДИС
	Тип документа: Паспорт гражданина РФ
	Номер документа: 2233112233
	Дата выдачи документа: 22.11.1997
	Тип отчета: 2225

Рис. 65

Необходимо проверить серийный номер сертификата, отображаемый в ошибке. Он должен совпадать с номером сертификата, который вы устанавливали.

Если он совпадает с номером сертификата, отображаемым в его свойствах, проверить, отображается ли сертификат в сертификатах в консоли mmc, в личных сертификатах локального компьютера.

Если сертификат виден в консоли (в личных сертификатах локального компьютера), перезапустить SSLGate и повторить запрос. Если ошибка повторилась, проверить, что при проверке, где установлен сертификат, у вас открыта консоль сертификатов именно локального компьютера и что сервис SSLGate запущен под локальным компьютером (в свойствах сервиса в закладке вход в систему).

Если сертификат не виден в консоли mmc (в личных сертификатах в локальном компьютере), то установить его («Панель управления - КриптоПро CSP - Сервис - Установить личный сертификат»). Подробнее – см. документацию по установке сертификатов. После установки перезапустить SSLGate.

Ошибка. Сертификат не найден. Certificate is not found



Информация о запросе	
Скачать xml-запрос	Номер: 98200
	Дата запроса: 12.10.2012 10:22:58
	Пользователь: admin
	Статус: Ошибка
	Ошибка: Ошибка подписи запроса(sign_errors)
	Текст ошибки: java.io.IOException: ssl gate error: certificate is not found: 1bbe9e58000200000000
	Запрос по: КОМОЛСОВ ЕВГЕНИЙ
	Тип документа: Паспорт гражданина РФ
	Номер документа:
	Дата выдачи документа: 26.01.2001
	Тип отчета: 2225

Рис. 66

Если данный сертификат установлен, необходимо проверить что установлены все корневые сертификаты и корневой сертификат, отображающийся на вкладке Path в свойствах сертификата (сертификаты должны быть установлены в доверенные корневые локального компьютера). Также такая ошибка возможна, если срок действия сертификата истек.

java.io.IOException: HTTP[S] remote request error: HTTP/1.1 403 Forbidden

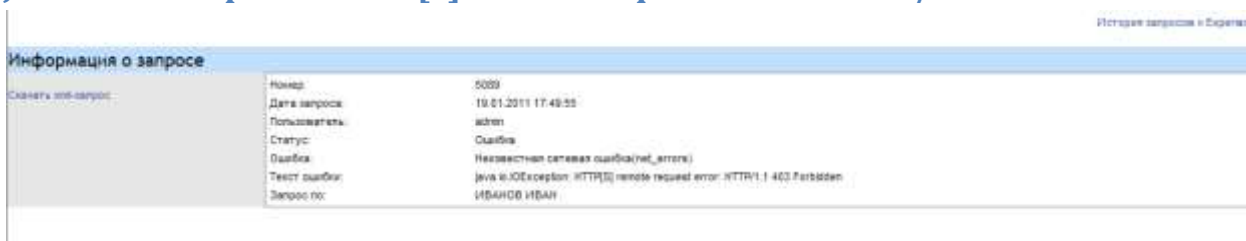


Рис. 67

Некорректно установлен личный сертификат, либо сертификат не указан в SSLGate.ini или указан некорректно, либо установлены не все корневые сертификаты, либо срок действия сертификата истек, либо сертификат не прописан на стороне ОКБ. Для коннектора EI - это самая распространенная ошибка и проверять нужно все сразу. Личный сертификат должен быть установлен в личных сертификатах локального компьютера, проверить это можно через консоль mms (пуск, выполнить, mms, консоль, добавить или удалить оснастку, сертификаты, компьютера, локального компьютера). Корневые сертификаты - файл cacert.p7b с сайта cрса20.cryptopro.ru - в консоли mms в закладке корневые сертификаты нужно сделать импорт этого файла. После переустановки сертификатов и изменения SSLGate.ini необходимо перезапустить SSLGate (как сервис)

Также такая ошибка может быть, если истекла триальная лицензия КриптоПро CSP. Как вариант, можно настроить коннектор ФМС с этим сертификатом, корректным адресом и некорректными логином/паролем и сделать запрос. При использовании сертификата на подпись ошибка обычно более информативная.

Ошибка. Код отчета 12 Расшифровка кода отчета: Структура XML запроса не корректна



Рис. 68

Возможные причины:

- 1) корректно установленный сертификат, но не вписан в список разрешенных на стороне Эквифакс
- 2) указан неправильный тип отчета
- 3) возможно структура XML некорректна.

Третий вариант наименее вероятен и сначала нужно проверить первые два.

java.io.IOException: HTTP[S] remote request error: HTTP/1.1 401 Unauthorized



История запросов в ЕИ

Информация о запросе		
Скачать XML-запрос:	Номер:	5096
	Дата запроса:	19.01.2011 18:18:28
	Пользователь:	admin
	Статус:	Ошибка
	Ошибка:	Неизвестная системная ошибка(net_error)
	Текст ошибки:	java.io.IOException: HTTP[S] remote request error: HTTP/1.1 401 Unauthorized
	Запрос на:	ЯНСИМТ ОАДМ

Рис. 69

Сертификат установлен корректно, но на стороне ЕИ ему не прописано разрешение на запросы. Проверить, что в SSLGate.ini указан текущий сертификат для запросов ЕИ, а не какой-то другой. Если это именно тот сертификат, которые вы получили в ЕИ, обратиться в ЕИ. Они должны прописать сертификат у себя как сертификат, с которым можно делать запросы.

Ошибка. Код отчета 50 при запросе в НБКИ



История запросов кредит

Информация о запросе		
Скачать XML-запрос:	Номер:	5096
	Дата отправления запроса:	19.01.2011 18:40:54
	Дата получения ответа:	19.01.2011 18:40:54
	Пользователь:	admin
	Статус:	ОК
	Запрос на:	ЯНСИМТ

Отчет НБКИ о кредитной истории субъекта		
Скачать отчет НБКИ как XML файл	Сообщения:	
Скачать отчет НБКИ как XML файл с подписью	Код: 50	Текст: Operation Not Authorized
Скачать XML-отчет в формате PDF		

Рис. 70

Надо проверять код участника в коннекторе. Если код участника НБКИ указан корректный, Вашу учетную запись для запросов в НБКИ заблокировали. (Предположительно - финансовая блокировка) Необходимо обратиться к менеджеру в НБКИ.

Ошибка. Код отчета 32. Текст: User Not Found



История запросов кредит

Информация о запросе		
Скачать XML-запрос:	Номер:	5511
	Дата отправления запроса:	20.01.2011 15:02:42
	Дата получения ответа:	20.01.2011 15:02:44
	Пользователь:	admin
	Статус:	ОК
	Запрос на:	МАКАЕДУНААРЫФФЕРБ

Отчет НБКИ о кредитной истории субъекта		
Скачать отчет НБКИ как XML файл	Сообщения:	
Скачать отчет НБКИ как XML файл с подписью	Код: 32	Текст: User Not Found
Скачать XML-отчет в формате PDF		

Рис. 71

Запрос дошел до НБКИ, НБКИ вернуло сообщение об ошибке. проверить логин (имя) в коннекторе НБКИ. Например, попробовать с ними залогиниться на сайте icrs.nbki.ru через браузер. Имя должно иметь формат 0101BV000001 – 4 символа, две буквы, 5 нулей и цифра. Имя отличается от кода участника на 1 или 2 последних символа. Одинаковым с ним быть не может.

Ошибка: 99 – нет полномочий

История запросов в Эквиф

Информация о запросе

Скачать xml-запрос:	Номер: 8018
	Дата запроса: 21.01.2011 10:29:43
	Пользователь: иван
	Статус: ОК
	Запрос по: МАКАКИНААЛЕКСАНДРА ПЕТРОВНА

Отчёт Experian

Скачать xml-ответ (xml)
Скачать xml-ответ с подписью
Скачать xml-ответ в формате pdf
Для печати

Ошибки

Код ошибки	Описание ошибки	Поле	Путь	Значение	Дополнительная информация
99	нет полномочий				

Рис. 72

Сертификат установлен корректно, запрос дошел до Experian и они вернули xml-ответ. В коннекторе ОКБ неверно указаны учетные данные (подписчик, группа, пользователь или пароль – все эти данные предоставляет ОКБ).

Или пользователь, указанный в настройках коннектора ОКБ, не имеет права осуществлять выбранный вид запроса, т.е. отсутствует доступ к определенной функции (functionNbr) со стороны бюро.

Ошибка: Такого отчета не существует

История запросов в Эквиф

Информация о запросе

Скачать xml-запрос:	Номер: 8033
	Дата запроса: 24.01.2011 12:50:48
	Пользователь: иван
	Статус: ОК
	Запрос по: ИВАНОВ ИВАН
	Тип документа: Паспорт гражданина РФ
	Номер документа: 4603123456
	Дата выдачи документа: 20.10.1993
	Тип отчета: 18

Ответ Эквифакс(ГПКС)

Для печати
Скачать xml-ответ
Скачать xml-ответ с подписью
Скачать отчет в формате pdf

ИВАНОВ ИВАН ИВАНОВИЧ. Паспорт России 4603123456 выдан 20.10.1993. Дата создания отчета: 24.01.2011 12:51:11

EQUIFAX®

Код отчета: 4
Расшифровка отчета: Такого отчета не существует
Дата создания отчета: 24.01.2011 12:51:11

Титульная часть

Фамилия, Имя, Отчество	ИВАНОВ ИВАН ИВАНОВИЧ
Дата и место рождения	20.10.1978 МОСКВА
Документ, удостоверяющий личность	Паспорт России 4603123456 выдан 20.10.1993 АЫА

Рис. 73

Проверить настройки коннектора (поле «Тип отчета»).

Они должны быть заполнены значениями, полученными в Equifax.

При необходимости банк должен уточнить у Equifax значение этих полей.

Статус: Ошибка

Ошибка: Ошибка подписи запроса (sign_errors)

Текст ошибки: java.io.IOException: ssl gate error: Getting signed BLOB size failed. Набор ключей не существует



История запросов к ЭСИА

Информация о запросе	
Имя и IP-адрес	
Номер:	8334
Дата запроса:	24.01.2011 13:03:34
Пользователь:	adme
Статус:	Ошибка
Ошибка:	Ошибка подписи запроса(sign_errors)
Текст ошибки:	java.io.IOException: ssl gate error: Getting signed BLOB size failed. Набор ключей не существует
Запрос по:	ИВАНОВ ИВАН
Тип документа:	Паспорт гражданина РФ
Номер документа:	468125458
Дата выдачи документа:	25.10.1993
Тип отчета:	IS

Рис. 74

Причина: сертификат установлен без привязки к закрытому ключу, либо привязка осуществлена, но ключ отсутствует, либо ключ хранится на токене и токен долго инициализируется.

Решение:

Зайти в консоль mms, зайти в личные сертификаты локального компьютера, выбрать нужный личный сертификат, нажать на него.

Проверить, есть ли надпись – «Есть закрытый ключ для этого сертификата».

Если надписи нет, установить сертификат (в локальное хранилище, в личные сертификаты) через «Панель управления - КриптоПро CSP – Сервис - Установить личный сертификат».

Если надпись есть, проверить, вставлен ли ключевой носитель.

В любом случае, рекомендуем сохранять закрытую часть в реестре и устанавливать сертификат с привязкой к реестру.

Запустить службу CreditRegistry SSLGate с параметром «Разрешить взаимодействие с рабочим столом», проверить, не появляется ли каких-либо сообщений на экране машины с SSLGate.

Ошибка Использован незарегистрированный сертификат подписи ("35e1320c0000000014f")

Причина: Сертификат не привязан к логину на стороне НБКИ.

Решение: Обратиться к менеджерам НБКИ.

Ошибка подписи запроса (sign_errors) java.net.SocketTimeoutException: Read timed out

Прописать максимальное время формирования ЭЦП (сек) в настройках коннектора 20 сек.

В свойствах сервиса SSLGate поставить галочку – разрешить взаимодействие с рабочим столом. Перезапустить сервис.

Повторить запрос.

Скорее всего, на машине с SSLGate будут сообщения на экране.

Если это запрос пароля – ввести пароль и нажать – сохранить.

Если это запрос ключевого носителя – необходимо проверить, что ключевой носитель с закрытой частью сертификата вставлен в компьютер (например, это может быть флешка\дискета\токен).

Рекомендуется копировать контейнер с закрытой частью в реестр и при установке сертификатов использовать привязку к реестру.

Также необходимо проверить настройки прокси Credit Registry.

Для SSLGateNet (версии SSLGate 3.0 и выше) должен быть открыт доступ к CRL.

Ошибка. Код отчета 28

The screenshot displays two main sections. The top section, titled 'Информация о запросе' (Request Information), contains a table with the following data:

Скачать оригинальный xml-запрос	Номер:	290862
Скачать оригинальный xml-запрос с подписью	Дата запроса:	10.10.2012 16:32:25
	Пользователь:	adm1n
	Статус:	OK
	Запрос по:	АБДУЛЛИН АБДУЛА
	Тип документа:	Паспорт гражданина РФ
	Номер документа:	99 01950455
	Дата выдачи документа:	27.12.2002
	Тип отчета:	2225

The bottom section, titled 'Ответ Эквифакс (ГПКС)' (Equifax Response), features the Equifax logo and the following text:

Код отчета: 28
Расшифровка кода отчета: Невозможно расшифровать запрос

Рис. 75

В настройках коннектора Эквифакс указан сертификат в поле «Серийный номер сертификата бюро Эквифакс». Необходимо отключить шифрование запроса (убрать сертификат из поля «Серийный номер сертификата бюро Эквифакс»).

Ошибка. Код отчета 49 при запросе в НБКИ

The screenshot displays two main sections. The top section, titled 'Информация о запросе' (Request Information), contains a table with the following data:

Скачать оригинальный xml-запрос:	Номер:	97698
	Дата отправления запроса:	10.10.2012 16:24:16
	Дата получения ответа:	10.10.2012 16:24:19
	Пользователь:	adm1n
	Статус:	OK
	Запрос по:	КОМОЛОВ

The bottom section, titled 'Отчет НБКИ о кредитной истории субъекта' (NBKI Report on Subject's Credit History), features the following text:

Сообщения:
Код: 49 Текст: User Not Authenticated

Рис. 76

проверить логин/пароль в коннекторе НБКИ. Например, попробовать с ними залогиниться на сайте icrs.nbki.ru через браузер.

Ошибка базы данных код ошибки -4 или -6: база данных не подключилась.

Проблемы на стороне ФМС. Попробуйте сделать запрос позже.

Превышено время ожидания ответа БКИ: read timeout

Информация о запросе	
Номер:	7677
Дата запроса:	31.01.2011 17:44:48
Пользователь:	admin
Статус:	Ошибка
Ошибка:	Превышено время ожидания ответа БКИ(timeout_errors)
Текст ошибки:	timeout_errors
Запрос по:	ИВАНОВА ТАТЬЯНА
Проверяемые данные:	Фамилия Иванова ; Имя Татьяна ;

Рис. 77

Либо бюро не вернуло ответ за "таймаут ожидания ответа БКИ", либо не поставлена галочка "сохранить пароль" при установке личного сертификата, либо запрос делался через прокси-сервер и доступа к сайту БКИ нет.

второй вариант нужно проверять только при определенных условиях!!

если:

- 1) ошибка вернулась по коннектору EI или BPC-direct
- 2) ошибка возвращается по всем запросам (т.е. по запросам по разным субъектам)
- 3) таймаут ожидания ответа от БКИ выставлен достаточный (не менее 60 сек)

в этом случае действительно может сработать таймаут ожидания ответа от БКИ, хотя реально SSLGate ждет ввода пароля.

это может произойти, если в свойствах сервиса SSLGate выставлена галочка "разрешить взаимодействие с рабочим столом"

и подключаются к машине с SSLGate по rdp (в этом случае окошко с запросом пароля "где-то" появляется, но на рабочем столе в rdp - не появляется). В этом случае нужно подключаться по rdp с консольной сессией (mstsc /admin)

в остальных случаях - таймаут ожидания ответа БКИ - это адекватный текст ошибки и нужно проверять таймаут в коннекторе.

Статус: Ошибка

Ошибка: Ошибка соединения с БКИ (bki_conn_errors)

Текст ошибки: ru.mbtc.creditregistry.sslgate.SslGateNegotiateException: SSLGate error: Connect SSL client handshake failed

После установки нового сертификата не перезапущена служба sslgate. Необходимо перезапустить службу.

Также возможно не установлены корневые сертификаты УЦ КРИПТО-ПРО, либо не перезапущен компьютер после установки КриптоПро CSP.

Если установка корневых сертификатов и перезапуск компьютера не помог, попробовать зайти на сайт <https://cpsa20.cryptopro.ru>

Если зайти не получилось, сделать (в произвольном порядке) следующее:

- обратиться в КристоПро (с вопросом, почему не получается зайти через IE на сайт <https://срса20.cryptopro.ru>)

- переустановить КристоПро CSP (удалить КристоПро CSP, перезагрузить компьютер, установить КристоПро CSP, перезагрузить компьютер)

Статус: Ошибка

Ошибка: Ошибка подписи запроса(sign_errors)

Текст ошибки: java.io.IOException: ssl gate error: Неправильный открытый ключ поставщика / The Keyset parameter is invalid

Номер:	104209
Дата запроса:	29.12.2012 11:09:29
Пользователь:	admin
Статус:	Ошибка
Ошибка:	Ошибка подписи запроса(sign_errors)
Текст ошибки:	java.io.IOException: ssl gate error: Неправильный открытый ключ поставщика.
Запрос по:	
Тип документа:	Паспорт гражданина РФ
Номер документа:	
Дата выдачи документа:	18.04.2002
Тип отчета:	2225

Рис. 78

Не сохранен пароль на контейнер с закрытой частью, к которой осуществлена привязка личного сертификата.

В настройках КристоПро CSP (вкладка сервис) необходимо изменить пароль с опцией «запомнить пароль» (в некоторых версиях КристоПро CSP есть возможность «протестировать контейнер», в этом случае также можно выставить опцию «запомнить пароль»).

Статус: Ок

Ошибка: Ошибка при разборе xml-ответа

номер:	995596
Дата отправления запроса:	12.06.2013 09:47:45
Дата получения ответа:	12.06.2013 09:47:49
Пользователь:	user
Статус:	ОК
Запрос по:	Вильченко

Ошибка при разборе xml-ответа (смотреть [лог](#)). org.xml.sax.SAXParseException, lineNumber: 1, columnNumber: 150, A DOCTYPE is not allowed in content.

Рис. 79

При запросах БРС (НБКИ-БРС). Сбой на стороне бюро, необходимо повторить запрос позднее.

MQ-ошибка в логe stdout: com.ibm.mq.MQException: MQJE001: An MQException occurred: Completion Code 2, Reason 2035

CRE не может подключиться к менеджеру очередей. Чаще всего это связано с неверными данными для аутентификации на сервере MQ или недостаточными правами.

1. Проверьте, что CRE использует набор jar-библиотек той же версии, что и сервер MQ.
2. В MQ существуют ограничения на длину имени пользователя. Какова длина имени пользователя, под которым запущена CRE?

- Если MQ развернута под Windows, то макс. длина не более 20 символов.
 - Если MQ развернута под Linux, то макс. длина не более 10 символов.
3. Если Вы отключили аутентификацию, то явно задайте MCA User ID на канале соединения с сервером. Нужно указать имя пользователя (или группы), обладающего достаточными правами на сервере MQ для работы с созданными менеджером очередей и очередями. Например, попробуйте указать группу *mqm*.

MQ-ошибка в логе stdout: org.codehaus.xfire.fault.XFireFault: Parameter {http://creditregistry.ru/2010/webservice/SingleFormatService}GroupRequestData does not exist!

1. Проверьте, какое значение Вы передаете в свойстве **CRE_SERVICE_NAME**. Если требуется вызвать web-сервис УСО, то CRE_SERVICE_NAME должно содержать значение *SingleFormatService*. По умолчанию CRE направляет поступающие сообщения на вход *ConnectorService*.
2. CRE_SERVICE_NAME передается, но CRE не может распознать значение данного свойства (в логах по-прежнему встречается запись “CRE_SERVICE_NAME: ConnectorService”). CRE использует интерфейс JMS для взаимодействия с очередями MQ. Проверьте значение свойства **mcd.Msd** в отправляемых сообщениях – оно должно быть *jms_text* или *jms_bytes*.

Примечание: для вывода в лог stdout заголовков и тела MQ-сообщений добавьте в настройки логирования CRE следующие строки:

```
ru.mbtc.creditregistry.mq.was.WsMqTimer=trace
ru.mbtc.creditregistry.mq.was.WsRequestExecuteTask=trace
```

С момента выпуска сертификата прошло больше года

The screenshot shows the Credit Registry web interface. At the top, there is a navigation menu with links like 'Администрирование', 'Регистрация', 'Запросы ТЦ', etc. Below the menu, there is a section titled 'Информация о запросе' (Request Information) with a table of details:

Номер:	34581
Дата запроса:	01.10.2013 16:48:58
Пользователь:	admin
Статус:	Ошибка
Запрос на:	НММСН/НМСР/ТЗТ9
Проверочные данные:	V81-код НММСН/НМСР/ТЗТ9 ; Серия и номер ПТС ; Номер двигателя ; Номер шасси ; Номер кузова

Below this is a section titled 'Отчет НБКИ по ТСЗ' (NBKI Report on TCZ). It contains a sub-section 'Общая информация' (General Information) with the following text:

Код ошибки НБКИ: 033
Текст ошибки НБКИ: С момента выпуска сертификата прошло больше года.

Below that is a sub-section 'Данные к проверке' (Data for check) with the following text:

V81-код: НММСН/НМСР/ТЗТ9
Серия и номер ПТС
Номер двигателя
Номер шасси
Номер кузова

Рис. 80

НБКИ разрешает использовать личный сертификат не более одного года. (несмотря на срок действия сертификата, прописанный в свойствах сертификата)

Нужно получить новый сертификат для запросов в бюро.

Код ошибки НБКИ 23 Проверка подписи не прошла

Общая информация

Код ошибки НБКИ 023
Текст ошибки НБКИ Проверка подписи не прошла.

Рис. 81

К пользователю (в настройках коннектора) не привязан сертификат, которым подписывается запрос. Если сертификат правильный, то нужно обратиться в НБКИ, чтобы пользователю, который прописан в коннекторе, прописали этот сертификат.

Wrong PIN was presented

Номер: 51445373
Дата запроса: 30.09.2013 09:23:15
Пользователь: HIGH
Статус: Ошибка
Ошибка: Ошибка подписи запроса(sign_errors)
Текст ошибки: java.io.IOException: ssl gate error: The card cannot be accessed because the wrong PIN was presented.

Предположительно, указан пароль на контейнер с сертификатом. Рекомендуется скопировать закрытую часть ключа в контейнер без пароля и установить сертификат с привязкой к контейнеру без пароля.

Ошибка: Ошибка соединения с БКИ(bki_conn_errors)

Текст ошибки: ru.mbtc.creditregistry.sslgate.SslGateNegotiateException: SSLGate error: Ошибка вызова SSPI, см. внутреннее исключение. (0x80004005):

Номер:	111281
Дата отправления запроса:	21.02.2014 11:01:17
Дата получения ответа:	21.02.2014 11:01:18
Пользователь:	admin
Статус:	Ошибка
Ошибка:	Ошибка соединения с БКИ(bki_conn_errors)
Текст ошибки:	ru.mbtc.creditregistry.sslgate.SslGateNegotiateException: SSLGate error: Ошибка вызова SSPI, см. внутреннее исключение. (0x80004005):
Запрос по:	КУСТОВ

Рис. 82

Указан пароль на контейнер с закрытой частью. Рекомендуется скопировать закрытую часть ключа в контейнер без пароля и установить сертификат с привязкой к контейнеру без пароля.

Так же данная ошибка может появиться после установки обновлений Windows, в этом случае необходимо переустановить КриптоПро CSP.

Ошибка: Ошибка подписи запроса (sign_errors): java.io.IOException: ssl gate error: Getting signed BLOB size failed. Function failed during execution.

Номер:	7516
Дата запроса:	14.03.2014 12:11:01
Пользователь:	admin
Статус:	Ошибка
Ошибка:	Ошибка подписи запроса(sign_errors)
Текст ошибки:	ru.mbtc.creditregistry.ssiGate.SsiGateSignException: java.io.IOException: ssl gate error: Function failed during execution.
Запрос по:	БОГДАНЧИК ВАДИМ

Рис. 83

Нужно проверять лицензию КриптоПро CSP, вероятнее всего истекла лицензия.

ПРИЛОЖЕНИЕ Н. Контакты для связи с БКИ

В данном разделе представлена контактная информация БКИ для получения учетных данных и сертификатов.

НБКИ – Национальное Бюро Кредитных Историй

<http://www.nbki.ru>

Тел.: +7 (495) 221-78-37

Техническая поддержка: Support@nbki.ru

Клиентская поддержка: AKurlykin@nbki.ru



ОКБ – Объединенное Кредитное Бюро

<http://www.bki-okb.ru/>

Тел.: +7 (495) 665-51-73

E-mail: msk@bki-okb.ru



Эквифакс Кредит Сервисиз

<http://www.equifax.ru/>

Тел. (тех. поддержка): +7 (495) 788-30-67

E-mail: office@equifax.ru



Кредитное бюро Русский Стандарт

<http://www.rs-cb.ru/>

Тел.: +7 (495) 609-64-24

E-mail: rscb@rs-cb.ru



ЦККИ – Центральный Каталог Кредитных Историй

<http://ckki.cbr.ru/>

Тел.: (495) 771-91-00

E-mail: webmaster@www.cbr.ru

